## Credo

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Welcome to the new home of the *InfoSec Perspective* column, a weekly commentary on information assurance (IA) topics.

To start the new series, I'd like to articulate some of the key ideas about writing on IA that I have accepted or developed in thirty years of work in the field.

To start with, the *InfoSec Perception* column is aimed primarily at programmers, analysts, network and security administrators, information security officers, security consultants, and C-level information executives (e.g., Chief Information Officers). However, beginners such as students are warmly welcomed and therefore technical jargon will be kept to a minimum; for example, all acronyms will be spelled out on first occurrence and their acronym defined at that time. Readers unfamiliar with basic concepts will be able to find definitions and articles easily online; more specialised concepts and terms will usually be defined or provided with explicit references.

I think that clear definitions of professional terminology are useful; for example, the Parkerian Hexad <

http://www.mekabay.com/courses/academic/norwich/is340/is340\_lectures/csh5\_ch03\_parkerian\_hexad.pdf > defined by Donn Parker in the 1980s and described in detail in his 1998 book, Fighting Computer Crime: A New Framework for Protecting Information (Wiley)< http://www.amazon.com/Fighting-Computer-Crime-Protecting-Information/dp/0471163783/ > provides a structure for experts to discuss the effects of security breaches with economy and clarity. Similarly, John D. Howard and Thomas A. Longstaff's "A Common Language for Computer Security Incidents" < http://www.cert.org/research/taxonomy\_988667.pdf > provides an excellent structure for clear delineation and discussion of the attackers, tools, vulnerabilities, actions, targets, unauthorized results and objectives of security breaches. The InfoSec Perceptions will include articles pointing to research and ideas that support common terminology and conceptual models.

The *InfoSec Perception* articles will rarely focus on news of the day, although sometimes readers will find references to recent events in a discussion of wider topics. This will be an educational series, not a news column. Incidents will be discussed to draw attention to principles that can improve security if readers think about their applicability to the systems for which they are responsible or even for their personal use of information technology. Some articles will focus on security information important to the general public and will urge readers to share their knowledge with family, friends, colleagues and schools.

Interdisciplinary research can provide valuable insights for IA – for example, a review of the implications of social psychology for IA<

http://www.mekabay.com/infosecmgmt/Soc Psych INFOSEC.pdf > opened up new approaches to implementing IA policies. This column will sometimes include discussions of topics in the

physical and social sciences, engineering, literature, history, and even music; all such discussions will bring to light ideas that can improve the practice of IA.

Humour can bring to light aspects of any subject that may be viewed as plebeian and boring. The *InfoSec Perception* will occasionally feature satire, fiction or even poetry if it makes a point about IA well for the readers.

For additional information about *InfoSec Perception*, see the Guidelines< **INSERT URL TO DOCUMENT 000\_rules.docx converted to HTML**> posted elsewhere on this site.

I hope that readers will learn from the column and will enjoy reading it.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

Copyright © 2011 M. E. Kabay. All rights reserved.

# Rules for InfoSec Perception

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

To guide readers and potential writers of the *InfoSec Perception*, the editors and I thought it would be useful to articulate our philosophy of writing in this new series. Here are some of the most important principles informing our publication:

- The *InfoSec Perception* is devoted to provoking thought about information assurance, not reporting on the latest events. This is not a news column: it's an educational column.
- The writing is intended to be clear, crisp, and easy to understand. We don't approve of long, complex sentences with unnecessary words, clichés, passive voice, and impersonal pronouns.
- Assertions of fact will be backed up with references to allow readers to
  - Learn more about the issue;
  - o Judge for themselves if the writer is portraying an issue fairly.
- Opinions will be indicated as such; for example, one might write, "It seems to me that...." or "In my experience, ...."
- Articles will often be co-authored by invited experts to provide a wide variety of Perceptions, not just those of the principal author. If someone writes to us with articulate arguments against a position that has been published in the column, we may invite them to publish an edited version of their comments in the column.
- No co-authored articles will be published without ensuring that the co-authors agree 100% with the edited content of the article.
- If we quote someone we have interviewed or heard, we'll send them the draft article to ask if they approve of the way we've represented their statements and will correct any errors before the material is published on our site.
- If authors choose to review publications or Web sites, negative reviews will be sent to the source of the publications and to those responsible for the Web sites being criticized, but they will not be published in the column. There are plenty of columns and blogs on the Web which provide almost nothing but criticism, but we will focus on highlighting useful and well-organized resources.
- If we do prepare articles critical of a point of view expressed by someone else or which criticize published statements, we will send to the authors of the disputed points for comment or rebuttal with at least a week of time before the article is sent in for publication.
- Comments on the Website will be posted only when commentators register with real (or real-sounding) names and provide an e-mail address for confirmation. No anonymous commentary will be accepted.
- Comments will be vetted for civility, but not for opinion. Vigorous articulation of fact and opinion is welcome, but *ad hominem* attacks (those focusing on the character of the targets rather than on ideas or performance) will be rejected.
- PDF versions of these columns will be archived by M. E. Kabay on his Website in an indexed folder after an appropriate delay (months).
- No one is permitted to post copies of these articles on any public Website without explicit

written permission (because multiple copies make it impossible to make corrections or updates to our columns). However, readers wishing to circulate electronic copies among colleagues, students, or friends at no cost are free to do so provided the original uniform resource locator (URL) is included in the circulated document.

We hope that you will enjoy reading the articles and thinking about the questions raised in these weekly columns. We look forward to a long and fruitful collaboration among writers, readers, and publishers.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

Copyright © 2011 M. E. Kabay. All rights reserved.

# Hurricane Andrew (August 1992): A Wake-up Call for Emergency Preparedness

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Recently I was asked to prepare a Webinar for the Master's in Public Administration < <a href="http://mpa.norwich.edu">http://mpa.norwich.edu</a> on lessons learned from Hurricane Andrew, the massive storm that devastated the Bahamas and other Caribbean islands and then hit the Florida coast with unparalleled intensity in August 1992.

The tropical storm that was to become Andrew was noticed in early August of 1992 and by August 17<sup>th</sup>, had been upgraded to the first named storm the season. Because the last major hurricane that had struck Florida was more than a generation before – in 1965 – few members of the public seemed concerned about it. But By August 22<sup>nd</sup>, Andrew was definitely a hurricane. By the time it passed the Bahamas on August 23<sup>rd</sup>, it was running at 150 mph. On that day, 700,000 residents of South Florida fled north in a disorganized panic; highways were clogged by panicked people in a desperate attempt to escape. In the meantime, Andrew reached extraordinary wind speeds near Miami – one recording topped out at 164 mph when the eye passed over Homestead, FL at 05:00 on August 24<sup>th</sup>.

In the three hours between 05:00 and 08:00 local time, Andrew moved across Florida, causing serious damage in Miami (e.g., downed trees, lamp posts and billboards) and almost completely devastated the Homestead and Florida City area a few miles to the southwest near the Everglades National Park.

The storm moved across the Gulf of Mexico on Aug 25<sup>th</sup> leaving residents in serious danger from exposure, lack of food and contaminated water. About 80,000 dwellings were destroyed; 250,000 people were homeless; a million people were without clean drinking water; and 1,500,000 people were without power. The storm reached the coast on August 26<sup>th</sup> and struck Louisiana, Alabama, Georgia and Tennessee with 140mph winds, although by that time it was starting to lose much of its force. Storm-spawned tornados rampaged through Louisiana, Alabama, Georgia and Tennessee destroying much of the sugar crop, destroying 10,000 homes and leaving 30 to 50 thousand residents homeless.

Government agencies and the private sector were faced with a massive cleanup. Unfortunately, recovery operations did not meet the expectations of the residents. Bickering among government officials irritated many observers and there were even outbreaks of looting. Although 8,000 National Guard troops and 27,000 active-duty US military personnel were eventually deployed, critics argued that the response had been poorly planned and executed. Government agencies, businesses and private citizens had simply not contemplated the need for advance planning and practice to cope with a storm of this magnitude.

A couple of years later almost to the day (August 13, 2004), Hurricane Charley found victims being supported quickly and efficiently by agencies such as the Federal Emergency Management Agency (FEMA< <a href="http://www.fema.gov/">http://www.fema.gov/</a>>). Officials in Florida and FEMA workers were generally praised< <a href="http://www.usatoday.com/weather/hurricane/2004-08-26-charley-fema\_x.htm">http://www.usatoday.com/weather/hurricane/2004-08-26-charley-fema\_x.htm</a>

> for the immediate distribution of ice, water and food door-to-door within the first 24 hours after the storm struck. Emergency communications were up and running at once and search-andrescue operations were effective. The first day of the disaster saw emergency toilets, air conditioning, tents, showers and medical emergency rooms in place.

In the next articles in this series, I'll look at specific lessons learned and practical recommendations for how to prepare for regional and national emergencies.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

Copyright © 2011 M. E. Kabay. All rights reserved.

# Hurricane Andrew (August 1992): Lessons Learned

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

In the preceding article in this column, I introduced some of the events of the great storm of 1992 that swept through the Caribbean and part of the south-eastern United States. Today I'll review some of the valuable lessons learned at that time and how they have improved emergency response in the decades since the early 1990s.

In the wake of the demolition of thousands of homes, a surprising issue cropped up: insurance. As attorney Gary A. Poliakoff, JD explained in his 2004 article, "Lessons of Andrew and Iniki: Adequate insurance and document safety are just two of the lessons emerging from Hurricanes Andrew and Iniki." < <a href="http://www.becker-">http://www.becker-</a>

poliakoff.com/pubs/articles/poliakoff g/lessons from andrew iniki.pdf > one of the key lessons from Andrew was that the insurance industry needed to be better prepared to cope with widespread damage. In the aftermath of the 1992 hurricane, policy holders discovered in too many cases that they did not understand the limitations of the policies they had been paying for – sometimes for years. Many found that insurance payments covered only a fraction of their recovery costs. As a result, government agencies worked with insurance providers to improve coverage and clarity – sometimes with regulations imposed by appropriate agencies.

Another failing that was uncovered – sometimes literally – by Hurricane Andrew was that slipshod construction causes terrible damage in storms like Andrew. Apparently some government regulators had fallen into cozy arrangements with local builders and failed to enforce even the limited standards that might have helped reduce damages and costs. The decisions by many insurance companies to declare bankruptcy or to terminate coverage for undamaged homes infuriated residents.

So what are some of the lessons that have become standard thinking in the wake of Andrew? The Master's of Public Administration program< <a href="http://mpa.norwich.edu">http://mpa.norwich.edu</a> at Norwich University<<a href="http://www.norwich.edu">http://www.norwich.edu</a> in Vermont includes two courses that bring students into detailed discussions of today's standards.

The BC511 course, "Continuity of Government Operations," is the first of two dealing with these essential matters; major topics include the following:

- Organizational analysis
- Risk and threat analysis
- Mitigation and control strategy development
- Implementing organizational structure

A necessary component of all business continuity programs is to understand clearly who does what and why in each organization. A culture of inclusion and free exchange is essential for successful planning and implementation.

Risk and threat analysis allows us to allocate resources rationally. Evaluate which components of the critical infrastructure your organization must coordinate with. Get to know the people in your areas of responsibility. Learn their priorities.

Look at a variety of threats and evaluate how each could affect the critical components of the systems for which you are responsible. Although you may not be able to derive precise probabilities for different types of damage, you can still get a sense of likelihood from published or historical records. Don't worry about imprecision – these probabilities are just part of a method for setting priorities.

#### The annualized loss expectancy, or ALE<

http://www.riskythinking.com/glossary/annualized\_loss\_expectancy.php >, is a useful tool for estimating (that is, doing better than just guessing wildly) at the level of investment appropriate to protect different components of the systems you are including in the business continuity and disaster recovery planning. In information security, however, we have to be aware that the enormous variety of equipment, software and configurations precludes the kind of precision that actuaries have achieved in classifying risks for, say, building types. Nonetheless, ALEs do provide an excellent basis for exploring options for rational allocation of resources. Sometimes we can learn enough about risks to engage in Monte Carlo Simulation<
http://www.palisade.com/risk/monte\_carlo\_simulation.asp > to arrive at overall probability distributions that we can constructively use in ALEs.

Whenever you are planning on changes to the usual way of doing business, remember that all organizations – including public agencies – are collections of *people* who have their own ideas, expectations and comfort zones. Don't just order people to change – discuss the issues and gain their support. Listen honestly and openly to what they have to say – after all, they are experts in their own work and actually know much more about the details than a manager from several levels above or from a different agency.

The second of the two courses in the MPA concentration in Continuity of Government Operations is BC521, "Incident Management and Emergency Response." Topics include

- Developing response plan
- Emergency operations centers
- Emergency communications
- Working with first responders
- Best practices for
- Developing off-site backups
  - Offsite work areas
  - o People and equipment for continuing operations

I'll look in more detail at these topics in the third of these columns.

For additional readings, see

- DHS (2011). "Critical Infrastructure." < http://www.dhs.gov/files/programs/gc\_1189168948944.shtm >
- Kabay, M. E. (2009). "Understanding Computer Crime Studies and Statistics, v6." < <a href="http://www.mekabay.com/methodology/crime\_stats\_methods.pdf">http://www.mekabay.com/methodology/crime\_stats\_methods.pdf</a> >
- Poliakoff, G. A. (2004). "Lessons of Andrew and Opal: Implementing a Disaster Plan."
   <a href="http://www.becker-">http://www.becker-</a>

- poliakoff.com/pubs/articles/poliakoff\_g/poliakoff\_lessons\_of\_andrew.pdf >
- US National Weather Service (1993). "Hurricane Andrew: South Florida and Louisiana: August 23-26, 1992." Available as e-book and on paper. < <a href="http://www.worldcat.org/title/hurricane-andrew-south-florida-and-louisiana-august-23-26-1992/oclc/29973581">http://www.worldcat.org/title/hurricane-andrew-south-florida-and-louisiana-august-23-26-1992/oclc/29973581</a>>

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

Copyright © 2011 M. E. Kabay. All rights reserved.

# Hurricane Andrew (August 1992): Organizational Issues

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

In the preceding articles in this column, I introduced some of the events of the great storm of 1992 that swept through the Caribbean and part of the south-eastern United States and reviewed some of the valuable lessons learned at that time and how they have improved emergency response in the decades since the early 1990s. Today, I'll continue with insights from the Master's of Public Administration program< <a href="http://mpa.norwich.edu">http://mpa.norwich.edu</a> at Norwich University< <a href="http://www.norwich.edu">http://www.norwich.edu</a> in Vermont, which includes two courses that bring students into detailed discussions of today's standards.

The second of the two courses in the MPA concentration in Continuity of Government Operations is BC521, "Incident Management and Emergency Response."

In developing a response plan, you can't plan for what you don't understand. And you can't expect to wait until you are perfect to have a plan! Critical path analysis<
http://www.mindtools.com/critpath.html > tells you what absolutely has to be done first and what gets done second and third. The critical path lays out which tasks depend on completing other priorities first. Politics has nothing to do with it: putting something first has to reflect absolute need and dependencies, not feelings of personal worth.

## Similarly, continuous process improvement<

http://www.processexcellencenetwork.com/process-management/ > , which is at the core of many US military organizational policies< http://www.armyobt.army.mil/about-continuous-process-improvement.html > defines thinking about how we work as a priority for everyone. One of the most frustrating responses anyone can receive in an organization after questioning why a procedure is in place is "Well, we've always done it that way." Every aspect of our work should be subject to rational thought, re-evaluation and improvement – and without having to worry that anyone is going to feel personally attacked when the someone raises possibilities for improvement, particularly in designing and refining incident response processes (IRP), business continuity plans (BCP), and disaster recovery plans (DRP). We must practice egoless work<a href="http://www.mekabay.com/nwss/435\_egoless\_work.pdf">http://www.mekabay.com/nwss/435\_egoless\_work.pdf</a> > as defined in Gerald Weinberg's famous text.

The organizational position of a person has nothing to do with the possibility of useful contributions for improvement; indeed those with hands-on, direct responsibility for accomplishing specific tasks may have more insight into what works and what doesn't work than managers at increasing degrees of remove from day-to-day operations.

Emergency Operations Centres (EOCs) are also called *command centres*, *situation rooms*, *war rooms*, and *crisis management centres*. These buildings, sections, or portable locations are where people can coordinate all the responses required to ensure smooth, effective delivery of appropriate responses to all aspects of an emergency. Fixed-position EOCs have to be built to withstand an appropriate level of stress (which should be predicated on historical information

about types of stress particular to a given location, such as earthquakes, floods, tornadoes, hurricanes and so on). It's no good having an EOC that blows away in a high wind – whether it's a permanent building or a mobile EOC constructed inside, say, a reinforced trailer that can be transported to an appropriate site using an 18-wheel tractor-trailer rig. Such mobile EOCs will be equipped with their own portable electric generators, mobile communications centres, and even pneumatic outriggers to stabilize the structures against high winds or post-earthquake temblors.<a href="http://www.directionsmag.com/articles/the-next-generation-emergency-operations-center-and-other-carnegie-mel/204433">http://www.directionsmag.com/articles/the-next-generation-emergency-operations-center-and-other-carnegie-mel/204433</a>

The EOC will also depend on an Incident Command System<

http://www.fema.gov/emergency/nims/IncidentCommandSystem.shtm > (ICS) that integrates computers, wireless and cabled networks, radio and mobile phones into a unitary system for effective management of operations. The EOC must help coordinate daily operational activities, including immediate communication between the EOC staff and personnel on the ground. Communications are central to success in all emergencies. Emergency radio systems are already in use by police and emergency response teams; remember that landline phones and often mobile phones may be severely disrupted in national disasters. An Event Information Tracking<a href="http://www.davislogic.com/EOC.htm#Event">http://www.davislogic.com/EOC.htm#Event</a> > (EIT) system provides audit trails to track all communications; these records give us the data we need for after-incident analysis, an essential part of continuous process improvement.

During the development of all IRP, BCP and DRP, practice is essential. These response plans are so complex that no one can predict which parts will work and which will fail. Using simulations< <a href="http://www.depiction.com/webinars/lanl">http://www.depiction.com/webinars/lanl</a> > can be helpful, but there's no substitute for practicing the actual operations (e.g., on a weekend) and recording as much as possible about the events using audio and video for post-mortem analysis. The US Federal Emergency Management Agency (FEMA) has suggestions</a> <a href="https://hseep.dhs.gov/pages/1001\_HSEEP7.aspx">https://hseep.dhs.gov/pages/1001\_HSEEP7.aspx</a> > for structuring such exercises.

Be aware that although trained first responders will be an essential and much-valued part of the plan, you will inevitably find volunteers – sometimes even from other countries – flying and driving in to help. Be prepared to use them wisely: the emergency is no time to have to stop and figure out what to do with these resources.

As for planning for your own agency's continued operations, you need backups of your data and your software that are kept away from the site you are protecting. You should think about storing such data in a different region from the area that could be affected by an emergency such as Hurricane Andrew. Some recovery sites are hundreds of miles away from the protected agencies.

You will have to think about what type of recovery site< <a href="http://docs.redhat.com/docs/en-US/Red Hat Enterprise Linux/4/html/Introduction To System Administration/s2-disaster-recovery-sites.html">http://docs.redhat.com/docs/en-US/Red Hat Enterprise Linux/4/html/Introduction To System Administration/s2-disaster-recovery-sites.html</a> > you need: cold sites are cheaper, but they take longer to get up and running. In contrast, hot sites may actually be usable for normal processing. The stock exchanges, for example, use all the computers in both their normal and their hot sites for processing – but each part can handle the full load without difficulty in case of emergency.

Where will people work if your main offices are inaccessible? Finding places for office workers is tricky. If you can afford to build spare work areas, great – but you may have to settle for searching out – in advance – alternate sites that will still support the level of electricity use, water, and communications you need. As for sharing resources with separate agencies, it's tough

to implement. Even if you can share hardware and software, how are you going to fit two offices of people into a single office if both are heavily used at all times? Can you work split shifts? If not, you're going to get into trouble.

Readers may wish to download and use "Supplement: Lessons from Hurricane Andrew" which is available as a narrated<

http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch57-58\_bcp-drp\_supplement\_andrew.pptx > PowerPoint file.

## For additional readings, see

- CDC "Emergency Preparedness & Response." < <a href="http://www.bt.cdc.gov/">http://www.bt.cdc.gov/</a> >
- DISA (2004). "Computer Incident Response Team Management CD-ROM." <a href="http://www.mekabay.com/infosecmgmt/disa\_cirtm\_cdrom.zip">http://www.mekabay.com/infosecmgmt/disa\_cirtm\_cdrom.zip</a>
- DHS "Critical Infrastructure." < http://www.dhs.gov/files/programs/gc\_1189168948944.shtm >
- FEMA "Are You Ready?" < <a href="http://www.fema.gov/areyouready/">http://www.fema.gov/areyouready/</a>>
- FEMA "Emergency Management Guide for Business & Industry." <a href="http://www.fema.gov/business/guide/index.shtm">http://www.fema.gov/business/guide/index.shtm</a> >
- FEMA "National Response Framework Resource Center." http://www.fema.gov/emergency/nrf/ >
- Kabay, M. E. (2011). "Backup." Lecture notes PPTX
   <a href="http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch57\_backups.pptx">http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch57\_backups.pdf</a>
- Kabay, M. E. (2011). "Business Continuity Planning." Lecture notes PPTX
   <a href="http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch58\_bc">http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch58\_bc</a>
   <a href="http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch58\_bc">http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch58\_bc</a>
   <a href="http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch58\_bc">http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch58\_bc</a>
   <a href="http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch58\_bc">http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch58\_bc</a>
   <a href="http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch58\_bc">http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch58\_bc</a>
   <a href="http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch58\_bc">http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch58\_bc</a>
- Kabay, M. E. (2011). "Computer Security Incident Response Team Management."
   Lecture notes
   <a href="http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch56\_csi\_rts.pptx">http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch56\_csi\_rts.pdf</a>
   <a href="http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch56\_csi\_rts.pdf">http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch56\_csi\_rts.pdf</a>
- MIT WORLD "Emergency Response" topics 
   <a href="http://mitworld.mit.edu/searches?term=emergency+response">http://mitworld.mit.edu/searches?term=emergency+response</a> >
- MIT WORLD "Disaster Recovery" topics
   <a href="http://mitworld.mit.edu/searches?term=disaster+recovery">http://mitworld.mit.edu/searches?term=disaster+recovery</a>>
- Ready.gov< <a href="http://www.ready.gov/">http://www.ready.gov/</a>>
- Weinberg, G. M. (1971). *The Psychology of Computer Programming*. Van Nostrand Reinhold (ISBN 0-442-29264-3). Xv + 288. Index. Still in print: Silver Anniversary Edition (1998)< <a href="http://www.amazon.com/Psychology-Computer-Programming-Silver-Anniversary/dp/0932633420">http://www.amazon.com/Psychology-Computer-Programming-Silver-Anniversary/dp/0932633420</a>>. See pp 52-60 in particular about egoless programming.

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

Copyright © 2011 M. E. Kabay. All rights reserved.

# HTCIA Membership Rules: A Debate

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

The High Tech Crime Investigation Association (HTCIA < <a href="http://www.htcia.org/">http://www.htcia.org/</a> is a respected organization to which I belonged until 2003, when I felt I had to resign according to the bylaws. The story – and a debate about HTCIA membership rules – comes out in a correspondence with Duncan Monkhouse <a href="http://ca.linkedin.com/pub/duncan-monkhouse/2/900/966">http://ca.linkedin.com/pub/duncan-monkhouse/2/900/966</a> >, President of the HTCIA for 2011. Mr Monkhouse has very kindly agreed to publish our correspondence.

## Mich Kabay to HTCIA:

Dear Colleagues,

I was an enthusiastic member of the HTCIA until I was hired by parents to investigate an accusation of unauthorized system access against their son at a private school. My investigation showed that the accusation was based on incorrect information and the case was dropped. I wrote about the situation as follows to a colleague in December 2003:

5) No member by virtue of their employment be in a position to represent or assist the defense in a criminal prosecution.

Belonging to an organization that prevents its members from "assisting the defense" is morally repugnant to me and should be a source of shame and embarrassment to the entire organization. It seems to me that the administration of justice in a society of laws depends absolutely on the impartial sharing of evidence and expertise with both prosecution and defense.

I urge the HTCIA membership to rethink their stand on this exclusionary rule.

In any case, I am certainly excluded from membership in the HTCIA, since my position as a professor and consultant makes me perfectly capable (and willing) to serve justice by aiding either the prosecution or the defense as required. This notice will serve as my resignation from the HTCIA effective immediately. I will be taking down the framed membership plaque from my wall with sincere regrets and will particularly miss the HTCIA list.<

Recently I received an announcement about a student poster competition sponsored by the HTCIA and I went to your site to see if conditions have changed. They have, but not for the better.

I looked at the current description of the HTCI < <a href="http://www.htcia.org/htcia">http://www.htcia.org/htcia</a> code.shtml >:

#### HTCIA Code of Ethics

I will support the objectives and purposes of the HTCIA, as stated in Article II of the Association Bylaws.

I agree to respect the confidential nature of any sensitive information, procedures, or techniques that I become aware of because of my involvement with the HTCIA.

I will not disclose such confidential material to anyone who is not a member in good standing of the HTCLA without the written permission from the HTCLA Board of Directors.

#### HTCIA Core Values

- (1) The HTCLA values the Truth uncovered within digital information and the effective techniques used to uncover that Truth, so that no one is wrongfully convicted!
- (2) The HTCLA values the Security of our society and its citizens through the enforcement of our laws and the protection of our infrastructure and economies.
- (3) The HTCLA values the Integrity of its members and the evidence they expose through common investigative and computer forensic best practices including specialized techniques used to gather digital evidence.
- (4) The HTCLA values the Trusted network of forensic and investigative professionals within private and public businesses including law enforcement who share our values and our vision.
- (5) The HTCLA values the Confidentiality of its membership and the information, skills and techniques they share within the association.

Then I looked at the Bylaws < <a href="http://www.htcia.org/bylaws.shtml">http://www.htcia.org/bylaws.shtml</a> >. This clause stands out for me:

5) Members may not, by virtue of their employment be in a position to represent or assist the defense in a criminal prosecution, unless < list of conditions >....

How do you reconcile Core Values (1) and Bylaws (5)?

\* \* \*

#### Duncan Monkhouse, President, HTCIA:

Professor Kabay,

Thank you for your email concerning the HTCIA code of ethics and bylaws. The sections that you drew my attention to were from the code of ethics:

The HTCLA values the Truth uncovered within digital information and the effective techniques used to uncover that Truth, so that no one is wrongly convicted!

and from the bylaws:

Members may not, by virtue of their employment be in a position to represent or assist the defense in a criminal prosecution, unless ...

You asked how HTCIA could reconcile the two, given the standard of impartiality to which reputable forensic examiners adhere. Our response is threefold:

First, the requirement of HTCIA members not to assist the defense is one that has been brought forward a number of times in recent years. Because of this, the bylaw section relating to defense work has been modified in some significant ways. These include allowing membership for court-appointed forensic examiners, as is the situation in the United States military and in some foreign countries. We also allow an HTCIA member to work for the defense, if the work is pro bono and the member receives chapter approval, or if the member is subpoenaed by the court.

That said, we ask the community to remember that HTCIA membership comprises a wide range of investigators in many roles, not just digital forensic examiners. We understand the argument that bringing together investigators for the prosecution and the defense promotes higher standards of evidence-gathering and thus due process. However, we do not believe that the current criminal legal system, which is adversarial by design, allows for the free exchange of information between those investigators. In a similar manner, I would not expect a defensive player to be allowed into the offensive huddle in a football game. All the players have the same goal of playing their best. But that does not allow for collaboration between opposing players on the field.

Finally, the goal of all investigators, forensic and otherwise, is to uncover the truth. To assist the people investigating high tech crimes, HTCIA provides a wide variety of training: an International Training Conference and Expo, regional conferences, and local Chapter meetings. We do not usually restrict who can attend the training.

HTCIA encourages its members to attend any relevant training from any source, including defense expert witnesses. HTCIA hopes that by providing the best possible training to the investigators of high tech crime that they are positioned to uncover the truth, to the best of their ability, and will thereby be able to present correct findings to prosecutors.

I hope that this has clarified HTCIA's position on our code of ethics and bylaws. If you have any further questions or comments please feel free to contact me.

\* \* \*

#### Mich Kabay to Duncan Monkhouse:

Dear Mr Monkhouse,

Thank you for your courteous and complete reply.

You wrote, "However, we do not believe that the current criminal legal system, which is adversarial by design, allows for the free exchange of information between those investigators. In a similar manner, I would not expect a defensive player to be allowed into the offensive huddle in a football game. All the players have the same goal of playing their best. But that does not allow for collaboration between opposing players on the field."

There is no question of collaboration on the specifics of a particular court case; just as you explain, the members of the opposing teams must not collude in preparing evidence.

However, there should be no question that all forensic investigators *must* benefit from the scientific, technical and methodological advances of our field. I would never forbid sports aficionados from discussing what kind of new footwear or shielding could improve performance and safety; would you and other members of the HTCIA advise against such information sharing? When a colleague publishes a

scholarly paper on the use of, say, EEG waves in an improved lie-detector, would you seriously propose that investigators should hide the information from others based on whether their principal roles are for defense and prosecution?

Would you approve of a technical security association in which anyone who works on penetration testing is to be excluded from membership because most of the members work on configuring intrusion prevention?

To me, the notion that contributing to defense efforts versus prosecution efforts defines two different categories of experts is an abomination. Defense and prosecution are *roles*, not defining attributes of a professional. A professional is not "infected" or "tainted" by working for the defense on contract; your own rules make it clear that the *only* factor determining exclusion is that a professional work for *fees* for the defense.

If it is necessary for members of the HTCIA to discuss a *specific* and *ongoing* legal case, that should be done outside the HTCIA under full control of applicable laws — otherwise there could be legal consequences. Otherwise, however, I see no benefit whatsoever in excluding members who happen to work for a defense team on contract.

I helped a defense team in a case involving gross negligence and incompetence in chain of evidence and chain of custody when a child was accused of criminal hacking in a school; that contract forced me to resign from the HTCIA. But my analysis saved a kid from prosecution based on an unjust accusation. Do I regret taking the case? Absolutely not. Do I regret that I had to leave the HTCIA? Sure – as you can see from my taking the time to argue with you even though I resigned in 2003!

\* \* \*

## **Duncan Monkhouse to Mich Kabay**

Thank you for providing me with your opinion on the matter of allowing people who work for the defense into HTCIA.

This is a thorny issue with many excellent arguments on each side. We do not disagree that "all forensic investigators *must* benefit from the scientific, technical and methodological advances of our field." This is why we do not, as mentioned, restrict defense experts from attending our training sessions, including our International Conference; we do not ask that our sponsors, or vendors do not aid or train the defense experts; and we do not prevent our members from sharing information with defense experts. We believe that these measures satisfy our core value of Truth as well as our bylaw requirement.

We have asked our membership a couple of times in the last few years about allowing defense experts to enroll as members, and the response has always been to maintain the status quo. We believe that this is largely because our investigator members come from many walks besides law enforcement and legal. They include regulatory agencies, corporate investigators and counsel, brand protection experts and auditors. They come from a variety of sectors including telecommunications, aerospace, utilities, transportation, manufacturing and food production, among others. Their work may involve some degree of digital forensics, but also includes intelligence-gathering, scientific research and old-fashioned legwork.

Thus many of our members are not comfortable with the presence of experts whose job it is to find reasonable doubt. In the course of due process, it is common for investigators to have questions about a particular tool or procedure they have not encountered before. We do not believe that any investigator

would deny the importance of a continuous learning process, but would not want that learning to be introduced as "doubt" that the investigator knows how to do his or her job. At no other point in the investigative process does a defense expert have pre-discovery access to the actions that compose due process, and we do not believe that we should provide it.

Again, we believe that our exclusions for military, foreign-country, pro-bono and other defense work more than adequately allow for the opposing side's perspective and experience, and we welcome the same perspective and experience at our training events.

Readers should feel free to respond to these ideas using the comment section of this blog.

\* \* \*

Duncan Monkhouse < <a href="http://ca.linkedin.com/pub/duncan-monkhouse/2/900/966">http://ca.linkedin.com/pub/duncan-monkhouse/2/900/966</a> > is President of the High Tech Crime Investigation Association (HTCIA < <a href="http://www.htcia.org/">http://www.htcia.org/</a> >). He has been serving as Electronic Evidence Officer for the Government of Canada since since 2001 and was an IT Security Consultant for the Government of Canada for nine years before that. He has also been the Manager of Specialized Computer Training at the Canadian Police College.

M. E. Kabay, < mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials. < http://www.mekabay.com/ >

Copyright © 2011 Duncan Monkhouse & M. E. Kabay. All rights reserved.

# News of the World Hacking Debacle: Groupthink in Action

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Starting in 2003, employees – including editors – of the now-defunct *News of the World* newspaper in Britain, controlled by Rupert Murdoch's News Corporation became embroiled in a series of scandals involving bribery of police officers, illegal access to telephone voicemail, dishonestly suing truthful news organizations for libel, lying to parliamentary and congressional investigating committees, and selecting noncompliant employees as scapegoats. I have provided a couple of references at the end of this week's column for readers seeking details.

The results of the illegal actions include the complete shutdown of the *News of the World*; the paper published its last edition on July 10, 2011 after 168 years of continuous publication. Two hundred people lost their jobs. In addition, a major corporate acquisition (that of BSkyB) by news Corporation was cancelled and a subsidiary, Wireless Generation, lost a contract with the government of New York State.

Such consequences seem to me to be comparable to those caused by criminal hackers and industrial spies. However, in this case, I think we are seeing the consequences of a sick corporate culture. Carl Bernstein<a href="http://www.thedailybeast.com/contributors/carl-bernstein.html">http://www.thedailybeast.com/contributors/carl-bernstein.html</a> >, is famous among people my age (and surely completely unknown to most of my undergraduate students, almost all of whom were born after 1990) for his reporting on the Watergate scandal<a href="http://www.washingtonpost.com/wp-srv/politics/special/watergate/">http://www.washingtonpost.com/wp-srv/politics/special/watergate/</a> > of the Nixon administration in the USA. Mr Bernstein wrote a commentary in July 2011 entitled "Murdoch's Watergate?"<a href="http://www.thedailybeast.com/newsweek/2011/07/10/murdoch-s-watergate.html">http://www.thedailybeast.com/newsweek/2011/07/10/murdoch-s-watergate.html</a> > in which he criticized the culture built by Murdoch:

- "Between the Post, Fox News, and the Journal, it's hard to think of any other individual who has had a greater [negative] impact on American political and media culture in the past half century."
- "Reporters and editors do not routinely break the law, bribe policemen, wiretap, and generally conduct themselves like thugs unless it is a matter of recognized and understood policy."
- "As one of his former top executives—once a close aide—told me, 'This scandal and all its implications could not have happened anywhere else. Only in Murdoch's orbit. The hacking at *News of the World* was done on an industrial scale. More than anyone, Murdoch invented and established this culture in the newsroom, where you do whatever it takes to get the story, take no prisoners, destroy the competition, and the end will justify the means."

The 2004 documentary "Outfoxed: Rupert Murdoch's War on Journalism," <a href="http://www.imdb.com/title/tt0418038/">http://www.imdb.com/title/tt0418038/</a> > directed and produced by Robert Greenwald <a href="http://www.robertgreenwald.org">http://www.robertgreenwald.org</a> > provides an inside look at a culture of enforced compliance with the extreme right-wing political views <a href="http://www.fair.org/index.php?page=1067">http://www.fair.org/index.php?page=1067</a> > of the

owners and upper executives of Fox News – a culture which converted a news organization into an effective propaganda machine< <a href="http://mediamatters.org/blog/201110190009">http://mediamatters.org/blog/201110190009</a> > not averse to printing doctored photographs< <a href="http://mediamatters.org/research/200807020002">http://mediamatters.org/research/200807020002</a> > of people it doesn't like< <a href="http://www.onthemedia.org/2008/jul/11/public-relations-retaliation/transcript/">http://www.onthemedia.org/2008/jul/11/public-relations-retaliation/transcript/</a> > that like Nazi anti-Semitic caricatures of the 1930s.

So how do these observations bear on information assurance?

I believe that any corporate culture which defines disagreement as treason is headed for disaster. As I wrote in "Social Psychology and INFOSEC: Psycho-Social Factors in the Implementation of Information Security Policy,"

http://www.mekabay.com/infosecmgmt/Soc\_Psych\_INFOSEC.pdf >

"In the extreme, a group can display groupthink, in which a consensus is reached because of strong desires for social cohesion. When groupthink prevails, evidence contrary to the received view is discounted; opposition is viewed as disloyal; dissenters are discredited. Especially worrisome for security professionals, those people in the grip of groupthink tend to ignore risks and contingencies. To prevent such aberrations, the leader must remain impartial and encourage open debate. Respected security consultants from the outside could be invited to address the group, bringing their own experiences to bear on the group's requirements. After a consensus—not the imposition of a dominant person's opinions—has been achieved, the group should meet again and focus on playing devil's advocate to try to come up with additional challenges and alternatives.

In summary, security experts should pay attention to group dynamics and be prepared to counter possible dysfunctional responses that interfere with acceptance of information assurance policies."

Preventing corruption at the heart of our enterprises is as essential as preventing intrusion by criminals and spies. If you are confronted with demand for illegal and unethical behaviour, challenge those making the demands. Don't risk your career by becoming involved in activities which will likely result in serious damage to all the stakeholders of your group.

Stand on principle or fall with the unprincipled.

## For Further Study:

- For a timeline of the scandals as of September 6, 2011, see "Phone hacking: timeline of the scandal" < <a href="http://www.telegraph.co.uk/news/uknews/phone-hacking/8634176/Phone-hacking-timeline-of-a-scandal.html">http://www.telegraph.co.uk/news/uknews/phone-hacking/8634176/Phone-hacking-timeline-of-a-scandal.html</a> > by Indu Chandrasekhar, Murray Wardrop and Andy Trotmanin *The Telegraph*.
- In addition, despite persistent debate about the reliability<
  <a href="http://concordia.academia.edu/ChituOkoli/Papers/375377/A">http://concordia.academia.edu/ChituOkoli/Papers/375377/A</a> Brief Review of Studies of Wikipedia In Peer-Reviewed Journals > of Wikipedia entries, there's an extensive summary <a href="http://en.wikipedia.org/wiki/News\_of\_the\_World\_phone\_hacking\_affair">http://en.wikipedia.org/wiki/News\_of\_the\_World\_phone\_hacking\_affair</a> > of the News of the World scandals in that collectively written compendium.
- If you would like to listen to a lecture for MSIA< <a href="http://infoassurance.norwich.edu">http://infoassurance.norwich.edu</a> students about social psychology (specifically organizational psychology), you can download a ZIP file</a> <a href="http://www.mekabay.com/courses/academic/norwich/msia/organizational">http://www.mekabay.com/courses/academic/norwich/msia/organizational</a> psychology p

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

Copyright © 2011 M. E. Kabay. All rights reserved.

## **Archive of NWSS Articles Now Online**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

As readers know from the introduction to this column, I published two articles a week for 11½ years as the *Network World Security Strategies* (NWSS) newsletter. As I have written elsewhere, the column was never intended to be a source of news; I'm an educator, not a journalist. Some of the articles are dated: they no longer refer to current issues or they have broken links and outdated references. However, many (I hope) are still useful in explaining principles of information assurance, offering guidance in practical matters of security and security management, or to help present security issues more amusingly than usual.

I'm pleased to report that I have finished putting every one of my NWSS articles online as a PDF devoid of advertising and generated index files to allow users to search quickly through the collection.

Readers can visit the archive< <a href="http://www.mekabay.com/nwss/">http://www.mekabay.com/nwss/</a> > for a descriptive page showing the options available.

- Readers may download individual files by consulting the file list
   <a href="http://www.mekabay.com/nwss/nwss\_list\_of\_files.htm">http://www.mekabay.com/nwss/nwss\_list\_of\_files.htm</a> where every file is named with a descriptive file name;
- The entire set of files is available in a single 10MB indexed PDF document< http://www.mekabay.com/nwss/nwss.pdf >;
- All the files, including individual PDFs, index files, and the consolidated PDF file are packed into two compressed files:
  - A ZIPX<http://www.mekabay.com/nwss/nwss.zipx > file for users who can unpack the current version of WinZip files;
  - A ZIP< <a href="http://www.mekabay.com/nwss/nwss.zip">http://www.mekabay.com/nwss/nwss.zip</a> > file for users limited to using older versions of WinZip files.

I invite everyone to use these documents freely for non-commercial purposes, which include

- Distributing individual articles or the entire collection within schools and other organizations for security awareness purposes;
- Passing material to social organizations to help non-technical people to learn some methods for protecting themselves against cybercrimes;
- Linking to individual files or to the directory on any Website.

However, there are specific restrictions that I impose on users of my freely-offered materials:

- Don't sell my stuff! I get *really mad* when I find anyone taking money from people for articles that I give away free (grrrr);
- Don't post my articles to *any* public Website or private intranet. I don't mind having individuals download their own copies of files, but posting copies on sites that distribute them to lots of people makes it difficult to fix errors in the original files I'd have to locate all the online copies to try to touch up the files.

I hope you will be able to use these materials in your work or just find those that entertain you.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

Copyright © 2011 M. E. Kabay. All rights reserved.

# **Virtual Meetings for IA Professionals**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

All of us involved in any kind of business may have to confer with our colleagues in real time, as opposed to the asynchronous communications supported by e-mail. However, it seems to me that traveling to professional meetings has become a burden, especially if the locations are far enough to warrant air travel. Airport security measures<

http://www.mekabay.com/opinion/airport\_safety.pdf > have increasingly approached Bruce Schneier's definition of security theatre< http://www.schneier.com/essay-292.html >, with recent complaints such as that of Jean Weber, whose 95-year-old, wheelchair-bound, incontinent mother "was asked to remove an adult diaper in order to complete a pat-down search."< http://www.nwfdailynews.com/articles/mother-41324-search-adult.html > Combined with the faltering world economy, the number of premium air travel (first class & last-minute bookings) declined sharply in 2011< http://www.travelpulse.com/iata-reports-sharp-decline-in-premium-air-travel.html >; but even ordinary air travel has continued to decline in recent years, leaving increasing numbers of empty seats and pushing airlines to increase their fares< http://www.marketwatch.com/story/surging-fuel-costs-hit-airline-stocks-2011-04-08 > for even stronger disincentives for business travel.

Virtual meetings using voice over Internet protocol (VoIP)<
<a href="http://voip.about.com/od/voipbasics/a/VoiceOverIP.htm">http://voip.about.com/od/voipbasics/a/VoiceOverIP.htm</a> provide options for businesses to reduce costs by eliminating physical travel. Hope Neel writes,

"Basically, there are three major types of conferencing, namely, teleconferencing or audio conferencing, video conferencing and web or internet conferencing. While audio conferencing solution is an all time hit for its not so high price and user-friendly features, web conferencing is deemed to be more interactive. All those seeking for a real time conference experience can find the solution in web conferencing call. It will enable them to access, share and exchange files as well as real time data."<
http://ezinearticles.com/?VoIP-Conference-Call-Solutions-For-Reduced-Operation-Cost-In-Your-Business&id=6097019 >

#### I've used the FreeConferenceCall<

http://www.freeconferencecall.com/prodfreeconferencecall.asp > phone conference service for several years and have consistently been happy with the service. Participants simply pay for their own telephone access to an assigned phone number; if everyone is in the same country and people have unlimited national calling, the call doesn't cost anything extra to anyone. The service can accept up to 96 callers for up to six hours – and it's easy to record the conference calls. The recordings can be accessed by phoning the conference number and punching in a code – or they can be downloaded for editing and posting on a Web server.

If your organization needs people in different countries to join a conference call, FreeConferenceCall even provides a service<
<a href="http://www.freeconferencecall.com/fcci/default.aspx">http://www.freeconferencecall.com/fcci/default.aspx</a> > where participants can call different incountry numbers to avoid international long-distance calls.

Recently, the company that runs FreeConferenceCall has introduced FreeScreenSharing< <a href="http://www.freescreensharing.com/index.html?promocode=FCC\_FSS2011">http://www.freescreensharing.com/index.html?promocode=FCC\_FSS2011</a> > which runs along the same lines: up to 96 participants can meet using audio conferencing, but in addition, they can all see the computer screen of the current host – and the host can be switched among participants at any time.

Some people are experimenting with meetings in virtual worlds (immersive visual environments) such as Second Life (SL)< <a href="http://secondlife.com/">http://secondlife.com/</a>>. Wagner James, writing in *New World Notes*,< <a href="http://nwn.blogs.com/nwn/">http://nwn.blogs.com/nwn/</a>> which is devoted to discussions of the technology and sociology of virtual worlds, reported in 2010 on the future of business meetings in virtual worlds.</a><a href="http://nwn.blogs.com/nwn/2010/04/virtual-meetings.html">http://nwn.blogs.com/nwn/2010/04/virtual-meetings.html</a> > He cited an expert on the subject, Erica Driver<<a href="http://www.thinkbalm.com/">http://www.thinkbalm.com/</a> > who commented that it might be a while before meetings in virtual worlds would appeal to a wide range of businesses.

Some of the professional groups who have been experimenting with professional meetings in virtual worlds include scientists. For example, William Sims Bainbridge wrote an article entitled, "The Scientific Research Potential of Virtual Worlds" <a href="http://www.sciencemag.org/content/317/5837/472.abstract">http://www.sciencemag.org/content/317/5837/472.abstract</a> > (membership or fee required for full text) in *Science* in July 2007. He pointed out that virtual worlds could provide a locus for collaboration among scientists and for acquisition of scientific knowledge:

"Virtual worlds such as SL provide environments and tools that facilitate creating online laboratories that can automatically recruit potentially thousands of research subjects, over a period of months, at low cost.... SL offers scripting and graphics tools that allow anyone to build a virtual laboratory building, functioning equipment to run the experiment, and incentives to motivate participation, such as giving each research subject a virtual helicopter to fly around SL .... It would be quite feasible to have advanced students replicate classic experiments inside SL, adding to our confidence in older results while giving young people valuable skills. Creative scientists may also be able to design experiments that are feasible in virtual worlds but were never possible before. For example, experiments can be done comparing the socioeconomic consequences of alternative government regulations, something next to impossible in society at large ..., perhaps taking advantage of the fact that issues of environmental pollution already loom large in WoW [World of Warcraft< <a href="http://us.battle.net/wow/en/">http://us.battle.net/wow/en/</a> | quests."

John Bohannon urged scientists to get involved in virtual worlds in his article, "Scientists, We Need Your Swords," < <a href="http://www.sciencemag.org/content/320/5874/312.2.full">http://www.sciencemag.org/content/320/5874/312.2.full</a> > in which he urged participation in "Convergence of the Real and the Virtual: The First Scientific Conference in the World of Warcraft 9-11 May" <

 $\frac{\text{http://convergentsystems.pbworks.com/w/page/16444397/May\%202008\%20Conference}}{2008. \text{ He reported} < \frac{\text{http://www.sciencemag.org/content/320/5883/1592.3.full}}{\text{conference with some glee, since at one participant was torn apart by a pack of hyenas – well, virtual hyenas – in the virtual world:}$ 

"Thus began the first scientific conference held in Azeroth, the online universe inhabited by millions of people playing World of Warcraft. Anyone who has been part of a conference's organizing committee knows that some glitches and mishaps are just unavoidable. And as usual, the problems that actually did occur were unforeseen. It was a success nonetheless. By the end of the third day, a real scientific exchange took place, I

married one of the conference participants, and within an hour of the wedding, we were all dead."

Merck Research Laboratories have been using a private world<
<a href="http://www.cio.com/article/638163/Online">http://www.cio.com/article/638163/Online</a> Collaboration How Merck Uses Virtual Worlds for Global Meetings > for business meetings using ProtoSphere<<a href="http://www.protonmedia.com/">http://www.protonmedia.com/</a> > starting in 2009. The organizers found that more than four-fifths of the 54 scientists at the first "virtual poster session in July 2009" were pleased with the experience. Some even commented that they were "more comfortable approaching senior scientists using their avatars than they would have been face-to-face." Writing about the findings, Stephanie Overby noted, "Other benefits included reduced travel costs, time savings and 'quick access to busy thought leaders who may not have otherwise been able to participate.""

A January 7, 2011 article in *Science* by John Bohannon entitled "Meeting for Peer Review at A Resort That's Virtually Free" http://www.sciencemag.org/content/331/6013/27.full.pdf > reported encouraging progress in the use of SL for National Science Foundation (NSF) http://nsf.gov/ prant reviews – a process that requires "More than 19,000 scientists [to] travel to NSF headquarters each year to take part in grant evaluation panels." For the US National Institutes of Health (NIH) http://nih.gov/ panels and "17,000 reviewers evaluated 61,000 proposals...." In the NSF trials, the scientists generally reported positive responses – and "all of the work was completed on time." The NSF pays Linden Lab http://lindenlab.com/ (creators of SL) only \$3,600 as a yearly rental fee for an "island" reserved for the NSF in SL; however, the virtual meetings "can save as much as \$10,000 per panel" – and there are thousands of review panels a year!

There are issues to consider, however, when organizing professional virtual meetings. James Shimabukuro< <a href="http://technologysource.org/author/james\_shimabukuro/">http://technologysource.org/author/james\_shimabukuro/</a> > wrote an excellent overview< <a href="http://technologysource.org/article/evolving\_virtual\_conference/">http://technologysource.org/article/evolving\_virtual\_conference/</a> > of concerns that must be addressed in planning and executing virtual meetings. One of the key problems that participants and organizers may encounter is that many participants may think that they don't have to reserve time for the meeting – unlike the sequestration that is common in physical "away" meetings – and find themselves being distracted by the quotidian demands of their normal work. Participating in virtual meetings may require self-discipline and the collaboration of colleagues. One of my colleagues who works in an office where there are no doors on the cubicles has a sign on her desk that she can prop up; it reads, "THE DOOR IS CLOSED."

Given that information assurance (IA) practitioners are usually at the forefront of technological change, I think it is time that our professional associations started experimenting with virtual worlds for our professional meetings.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:mekabay@gmail.com">http://www.mekabay.com/</a> >

Copyright © 2011 M. E. Kabay. All rights reserved.

Permission is hereby granted to InfoSec Reviews to post this article on the InfoSec Perception

Web site in accordance with the terms of the Agreement in force between <i>InfoSec Reviews</i> and M. E. Kabay.

# Ira Winkler is Wrong: Undergraduate Degrees in Information Assurance are Worthwhile

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Ira Winkler, a respected information assurance professional – and a long-time colleague starting in the early 1990s, when we were both involved with the National Computer Security Association – recently wrote, "Let's scuttle cybersecurity bachelor's degree programs." (November 9, 2011, *Computerworld*) <

http://www.computerworld.com/s/article/9221668/Let s scuttle cybersecurity bachelor s degree programs >. Since I was responsible for creating the original Bachelor of Science in Computer Security and information Assurance (BSCSIA<

<a href="http://programs.norwich.edu/business/csia/">http://programs.norwich.edu/business/csia/</a> ) program at Norwich University<a href="http://www.norwich.edu">http://www.norwich.edu</a> , I'm well suited to present a friendly rebuttal of his analysis.

## 1 Computer security undergraduate degrees too specialised?

Winkler writes,

"In no other computing discipline do you have a specialized degree program. You do not earn a bachelor's degree specifically in software engineering, computer graphics, artificial intelligence, database management, systems administration, Web applications programming or project management."

Yes, you do. It took me 30 seconds with GOOGLE to find lots of useful links. For example, here's the definition of the bachelor of science in software engineering from the National Center for Education Statistics CIP Code 14.0903.<

http://nces.ed.gov/ipeds/cipcode/cipdetail.aspx?y=55&cipid=87307 >

"Definition: A program that prepares individuals to apply scientific and mathematical principles to the design, analysis, verification, validation, implementation, and maintenance of computer software systems using a variety of computer languages. Includes instruction in discrete mathematics, probability and statistics, computer science, managerial science, and applications to complex computer systems."

The "AllEngineeringSchools" database< <a href="http://www.allengineeringschools.com/engineering-degree/all-degrees/">http://www.allengineeringschools.com/engineering-degree/all-degrees/</a> provides easy access to links for colleagues and universities offering bachelor's degrees in

- Application Development
- Database Management
- Game & Simulation Programming

- Game Programming
- Health Informatics
- Information Security And Forensics
- Information Systems Management
- Mobile Computing
- Network Administration
- Network Management
- Project Management
- Security
- Software Engineering
- Software Systems Engineering
- Visual & Game Programming
- Web Development.

So there are *indeed* specialized bachelor's degrees in computer-science related areas, and one of those areas is information assurance.

## 2 "Why should there be a bachelor's degree specific to cybersecurity?"

Winkler answers that a question himself:

"Security professionals need to function in a variety of disciplines. They can be called upon to evaluate software for security vulnerabilities, to determine whether a user interface is suffering from information leakage, to design secure databases, to secure operating systems, to assess and shore up the security of websites, to incorporate security requirements into new developments and so on. The person you ask to do all of those things needs to be well rounded."

#### Then he stumbles:

"But a cybersecurity degree program offers many security classes at the expense of classes that would normally be required to get a general degree in computer science or information systems."

That's certainly not true of the BSCSIA at Norwich University. The curriculum is shown on our Web site< <a href="http://programs.norwich.edu/business/csia/curriculum/">http://programs.norwich.edu/business/csia/curriculum/</a> > as is that of the Bachelor of Science in Computer Science</a> <a href="http://programs.norwich.edu/business/computerscience/">http://programs.norwich.edu/business/computerscience/</a> >. Figure 1 shows the similarities and differences of the two programs:

Figure 1. Comparison of BSCS & BSCSIA programs at Norwich University.

Data Structures Databases Discrete Math Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems Information Assurance I Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Management of Organizations Management of Organizations Number Theory Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	Arts & Humanities Elective Business Law I Business Law II Business & Economic Statistics 1  Composition & Literature I Composition & Literature II  Computer Programming I Computer Programming II  Concentration Capstone I Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networking Data Structures
Business Law I Business & Economic Statistics 1 Business & Economic Statistics 1 Business & Economic Statistics 1 Calculus II Composition & Literature I Composition & Literature II Composition & Literature II Computer Architecture Computer Organzation & Programming Computer Programming I Computer Programming II Contemporary Issues in Computer Science Concentration Capstone I Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Structures Data Structures Databases Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems Information Assurance I Information Assurance I Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Number Theory Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	Business Law I Business Law II Business & Economic Statistics 1  Composition & Literature I Composition & Literature II  Computer Programming I Computer Programming II  Concentration Capstone I Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networking Data Structures Databases
Business & Economic Statistics 1 Business & Economic Statistics 1 Calculus II Calculus II Composition & Literature I Composition & Literature II Composition & Literature II Computer Architecture Computer Organzation & Programming Computer Programming I Computer Programming II Computer Programming II Contemporary Issues in Computer Science  Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networki Data Structures Databases Discrete Math Discrete Math Discrete Math Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems  Information Assurance I Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Number Theory Operating Systems  Precalculus Principles of Accounting *or* Principles of Economics (Micro)  Precalculus Principles of Accounting *or* Principles of Economics (Micro)	Business Law II Business & Economic Statistics 1  Composition & Literature I Composition & Literature II  Computer Programming I Computer Programming II  Concentration Capstone I Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networking Data Structures Databases
Business & Economic Statistics 1 Calculus I Calculus II Composition & Literature I Composition & Literature II Composition & Literature II Composition & Literature II Computer Architecture Computer Organzation & Programming Computer Programming I Computer Programming II Contemporary Issues in Computer Science  Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networki Data Structures Data Structures Databases Discrete Math Discrete Math Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems  Information Assurance I Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Macroeconomics Management of Organizations Number Theory Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	Composition & Literature I Composition & Literature I Composition & Literature II  Computer Programming I Computer Programming II  Concentration Capstone I Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networking Data Structures Databases
Calculus I Calculus II Composition & Literature I Composition & Literature II Composition & Literature II Composition & Literature II Composition & Literature II Computer Architecture Computer Organzation & Programming Computer Programming I Computer Programming II Computer Programming II Concemporary Issues in Computer Science  Concentration Capstone I Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networki Data Structures Data Structures Data Structures Databases Discrete Math Discrete Math Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems  Information Assurance I Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Macroeconomics Management of Organizations Number Theory Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	Composition & Literature I Composition & Literature II  Computer Programming I Computer Programming II  Concentration Capstone I Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networking Data Structures Databases
Composition & Literature I Composition & Literature II Composition & Literature II Computer Architecture Computer Organzation & Programming Computer Programming I Computer Programming II Contemporary Issues in Computer Science  Concentration Capstone II Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networki Data Structures Databases Discrete Math Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems  Information Assurance I Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Management of Organizations Number Theory Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)  Computer Programming I Computer Programming II Computer Programing II Concentration Capstone I Concentration Capstone I Concentration Capstone I Concentrat	Composition & Literature II  Computer Programming I  Computer Programming II  Concentration Capstone I  Concentration Capstone II  Cryptology  Cyberlaw and Cybercrime  Data Communications and Networking  Data Structures  Databases
Composition & Literature II Computer Architecture Computer Organzation & Programming Computer Programming I Computer Programming II Computer Programming II Contemporary Issues in Computer Science  Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networki Data Structures Databases Discrete Math Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems  Information Assurance II Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Management of Organizations Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)  Precalculus Principles of Accounting *or* Principles of Economics (Micro)	Composition & Literature II  Computer Programming I  Computer Programming II  Concentration Capstone I  Concentration Capstone II  Cryptology  Cyberlaw and Cybercrime  Data Communications and Networking  Data Structures  Databases
Composition & Literature II Computer Architecture Computer Organzation & Programming Computer Programming I Computer Programming II Contemporary Issues in Computer Science  Concentration Capstone II Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networki Data Structures Databases Discrete Math Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems  Information Assurance II Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Management of Organizations Number Theory Operating Systems  Precalculus Principles of Accounting *or* Principles of Economics (Micro)  Computer Programming I Computer Programming II Concentration Capstone II	Composition & Literature II  Computer Programming I  Computer Programming II  Concentration Capstone I  Concentration Capstone II  Cryptology  Cyberlaw and Cybercrime  Data Communications and Networking  Data Structures  Databases
Computer Architecture Computer Organzation & Programming Computer Programming I Computer Programming II Computer Programming II Contemporary Issues in Computer Science  Concentration Capstone I Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networki Data Structures Databases Discrete Math Discrete Math Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems Information Assurance I Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Management of Organizations Number Theory Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)  Microeconomics (Micro)	Computer Programming I Computer Programming II  Concentration Capstone I Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networking Data Structures Databases
Computer Programming I Computer Programming II Concentration Capstone I Concentration Capstone II Co	Computer Programming II  Concentration Capstone I Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networking Data Structures Databases
Computer Programming II Contemporary Issues in Computer Science  Concentration Capstone I Concentration Capstone II Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networki Data Structures Data Structures Databases Discrete Math Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems  Information Assurance I Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Management of Organizations Number Theory  Operating Systems  Precalculus Principles of Accounting *or* Principles of Economics (Micro)	Computer Programming II  Concentration Capstone I Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networking Data Structures Databases
Contemporary Issues in Computer Science  Concentration Capstone I Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networki Data Structures Data Structures Databases Discrete Math Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems Information Assurance I Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Macroeconomics Management of Organizations Number Theory Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	Concentration Capstone I Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networking Data Structures Databases
Concentration Capstone I Concentration Capstone II Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networki Data Structures Data Structures Databases Discrete Math Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems Information Assurance I Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Macroeconomics Management of Organizations Number Theory Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networking Data Structures Databases
Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networki Data Structures Databases Discrete Math Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems Information Assurance I Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Management of Organizations Management of Organizations Number Theory Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	Concentration Capstone II Cryptology Cyberlaw and Cybercrime Data Communications and Networking Data Structures Databases
Cryptology Cyberlaw and Cybercrime Data Communications and Networki Data Structures Data Structures Databases Discrete Math Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems Information Assurance I Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Management of Organizations Management of Organizations Number Theory Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	Cryptology Cyberlaw and Cybercrime Data Communications and Networking Data Structures Databases
Cyberlaw and Cybercrime Data Communications and Networki Data Structures Data Structures Databases Discrete Math Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems Information Assurance I Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Management of Organizations Management of Organizations Number Theory Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	Cyberlaw and Cybercrime Data Communications and Networking Data Structures Databases
Data Communications and Networki Data Structures Databases Discrete Math Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems Information Assurance I Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Management of Organizations Management of Organizations Number Theory Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	Data Communications and Networking Data Structures Databases
Data Structures Databases Discrete Math Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems Information Assurance I Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Management of Organizations Management of Organizations Number Theory Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	Data Structures Databases
Databases Discrete Math Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems Information Assurance I Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Management of Organizations Management of Organizations Number Theory Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	Databases
Discrete Math Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems Information Assurance I Information Assurance II Intro to Psychology Macroeconomics Management of Organizations Management of Organizations Management of Organizations Number Theory Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	
Discrete Math Foundations of Computing & Security Fundamentals of Digital Systems  Information Assurance I Information Assurance II Intro to Psychology  Macroeconomics Management of Organizations Management of Organizations Management of Organizations Number Theory  Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	Foundations of Computing & Security
Foundations of Computing & Security Fundamentals of Digital Systems  Information Assurance I Information Assurance II Intro to Psychology  Macroeconomics Management of Organizations Management of Organizations Management of Organizations Number Theory  Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	Foundations of Computing & Security
Fundamentals of Digital Systems  Information Assurance I Information Assurance II Intro to Psychology  Macroeconomics  Management of Organizations  Management of Organizations  Management of Organizations  Number Theory  Operating Systems  Precalculus  Principles of Accounting *or* Principles of Economics (Micro)	Foundations of Computing & Security
Information Assurance I Information Assurance II Information Assurance II Intro to Psychology  Macroeconomics Management of Organizations Management of Organizations Number Theory  Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	
Information Assurance II Intro to Psychology  Macroeconomics Management of Organizations Management of Organizations Management of Organizations Number Theory  Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	
Intro to Psychology  Macroeconomics  Management of Organizations  Management of Organizations  Management of Organizations  Number Theory  Operating Systems  Precalculus  Principles of Accounting *or* Principles of Economics (Micro)	1 111 111
Macroeconomics  Management of Organizations  Management of Organizations  Management of Organizations  Number Theory  Operating Systems  Precalculus  Principles of Accounting *or* Principles of Economics (Micro)	
Management of Organizations  Macroeconomics  Management of Organizations  Number Theory  Operating Systems  Precalculus  Principles of Accounting *or* Principles of Economics (Micro)	Intro to Psychology
Management of Organizations Number Theory Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	
Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	
Operating Systems Precalculus Principles of Accounting *or* Principles of Economics (Micro)	
Precalculus Principles of Accounting *or* Principles of Economics (Micro)	Number Theory
Principles of Accounting *or* Principles of Economics (Micro)	Dwagalaulua
Prog. Languages	offics (Micro)
Organizational Behavior	Organizational Robavior
Public Speaking	
Software Engineering I Software Engineering I	
Software Engineering II Software Engineering II	
Software Engineering III	Software Engineering II
Technical Writing	Technical Writing
University Physics I Lab Science I	
University Physics II Lab Science II	
omversity in yoles in	and selence if
Electives:	
Concentration Elective	Concentration Flective
Concentration Elective  Concentration Elective	
Concentration Elective	
Concentration Elective	
Concentration Elective	
Concentration Elective	
Free Elective	
History Elective History Elective	
Literature Elective Literature Elective	•
Lab Sci Elective	
Math Elective	
Humanities/Arts. Elective	
Humanities/Social Sciences Elective	
Humanities/Social Sciences, Elective	

Figure 2. Concentration Requirements for BSCSIA at Norwich University.

FORENSICS CONCENTRATION		ADVAN	ADVANCED INFOSEC CONCENTRATION	
CJ442	Digital Forensics	CJ442	Digital Forensics	
IS311	Network Forensics	CP431	Network Security	
IS312	Malware Forensics	EE325	Computer Architecture & Operating Systems	
IS411	Digital Investigation	IS440	Software Engineering III	
	Concentration Elective		Concentration Elective	
	Concentration Elective		Concentration Elective	

#### Concentrations:

Figure 3 shows which courses are allowed to fulfil elective requirements in the BSCSIA program.

Figure 3. Electives permitted for BSCSIA concentraitons at Norwich University.

Permit	ted Concentration Electives	Available for	
		Forensics	INFOSEC
CP431	Network Security	Y	
EE325	Computer Architecture & Operating Systems	Y	
IS300	Management Information Systems	Y	Y
IS311	Network Forensics		Y
IS312	Malware Forensics		Y
IS330	Ethics in Computing & Technology	Y	Y
IS370	Introduction to Information Warfar	Y	Y
IS380	Offensive Information Warfare	Y	Y
IS382	Defensive Information Warfare	Y	Y
IS406	Special Topics in Computer Science	Y	Y
IS407	Politics of Cyberspace	Y	Y
IS410	Computing Internship	Y	Y
IS411	Digital Investigation		Y
IS440	Software Engineering III	Y	
PY234	Forensic Psychology	Y	Y

I fully agree with Winkler that "The best college degrees strive to help people have a broad understanding of not just their field, but culture in general." Surely most security experts will agree that the Norwich BSCSIA degree is indeed a multidisciplinary program. Norwich BSCSIA graduates have consistently attained positions of responsibility in their organizations; our students are widely recognized as having a thorough foundation that allows them to listen, learn, analyse, and communicate at high levels of achievement.

## 3 Baccalaureate holders lack experience

Winkler writes,

"When you come right down to it, though, there is little in the world of information security that is more valuable than experience. And new graduates nearly always lack it to any significant degree."

In the first place, the importance of experience does not vitiate academic preparation.

In the second place, although I cannot speak for other schools, I do know that many Norwich BSCSIA students have had excellent opportunities for real-world experience. For example, 15 students are currently (Fall 2011) taking a system administration course to qualify for their paid work in the Norwich University Center for Advanced Computing and Digital Forensics (NUCAC-DF< <a href="http://www.nuacc.org/">http://www.nuacc.org/</a>>).

Many (I don't know exactly how many) students find work during the summers; they often use their experience to good effect in their job-hunting and in class. And since about three quarters of our students are Cadets< <a href="http://www.norwich.edu/cadets/index.html">http://www.norwich.edu/cadets/index.html</a> > in the Reserve Officer Training Corps (ROTC< <a href="http://www.norwich.edu/cadets/rotcrequirements.html">http://www.norwich.edu/cadets/rotcrequirements.html</a> >) at Norwich, many of them work in military assignments during their off-terms. I have had students who came back from assignments involving COMSEC<

www.dtic.mil/whs/directives/corres/pdf/852301p.pdf > in the US military and civilians who have worked on SIGINT< <a href="http://www.nsa.gov/sigint/index.shtml">http://www.nsa.gov/sigint/index.shtml</a> > with the National Security Agency (NSA< <a href="http://www.nsa.gov/">http://www.nsa.gov/</a> >). These students consistently contribute valuable insights to the other students based on their experience in real working environments.

In addition to self-arranged internships, we even have records of 14 students since 2000 who actually *paid* to take the IS410 "Computing Internship" course (Course Descriptions< <a href="http://www.norwich.edu/about/policy/academic/archive-universityCatalog/2010-2011/universityCatalog-courses1011.pdf">http://www.norwich.edu/about/policy/academic/archive-universityCatalog/2010-2011/universityCatalog-courses1011.pdf</a> >, page 278) formally so it could be added to their academic transcript. IS410 is routinely used to provide an academic vehicle for students who receive internships in private industry and government agencies:

Internships within CS/CSIA are designed to provide computing majors with the opportunity to apply and expand their knowledge within the computing discipline. The student must be a junior or senior at the time of enrollment[sic] and have good academic standing. The student must have the internship approved beforehand by a faculty member in CS/CSIA and have the written consent of the CS/CSIA Program Coordinator. In addition, a supervisor within the sponsoring organization must agree to provide a written description of the internship beforehand, and provide progress reports during and after the internship experience....

I don't know how to quantify Ira Winkler's assertion that "...new graduates nearly always lack it [experience] to any significant degree." However, I try to avoid fuzzy phrases such as "nearly always" and "to any significant degree" in describing *any* phenomenon.

## 4 Professors' Field Experience

On a secondary level, there is an indirect effect on our students from the field experience of our faculty. Every one of our computer security professors has real-world experience earning their living at what they teach. Some of the themes in all of the guidance our faculty include in their courses are

- Study to make your learning a permanent part of how you look at the world, not just isolated information that you use to pass an exam and then forget.
- Learn all the time: you can't stop and sit on your behind in any profession and certainly not in the world of information technology and information assurance.
- Information assurance is a servant to the organization: we help our colleagues achieve reasonable goals for protecting assets and stakeholders. We don't dictate, we collaborate.
- Security is a goal, not a state: you are facing moving, evolving threats.
- When you start work, shut up and listen: don't swagger around issuing arrogant commentaries. Only after you have earned the respect of your colleagues should you venture to make suggestions for improvement politely!
- Communicate clearly and simply and respect word limits and deadlines in your professional assignments.

Finally, our Dean just informed us that every one of our fourth-year BSCSIA students now has a job offer, multiple job offers, or a signed contract of employment for their graduation in May 2012.

\* \* \*

I hope that readers will find this analysis helpful in evaluating Mr Winkler's comments – and that readers won't be quite as depressed about the state of information assurance education as Mr Winkler is.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

Copyright © 2011 M. E. Kabay. All rights reserved.

## All We Want are the Facts, Ma'am

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Has anyone ever muttered, "Just the facts" to you and explained that it was a catch-phrase used by Jack Webb< <a href="http://www.imdb.com/name/nm0916131/">http://www.imdb.com/name/nm0916131/</a> > in his character as Sergeant Joe Friday in the 1950s television series, "Dragnet?" <a href="http://www.imdb.com/title/tt0043194/">http://www.imdb.com/title/tt0043194/</a> >

## **Snopes**

You may know that a good source for checking such a claim is Snopes< <a href="http://www.snopes.com">http://www.snopes.com</a> >, which publishes careful analysis of all manner of information circulating in the popular culture, including through chain e-mail letters. Authors Barbara and David Mikkelson write<<a href="http://www.snopes.com/radiotv/tv/dragnet.asp">http://www.snopes.com/radiotv/tv/dragnet.asp</a> > that Joe Friday *never* said "Just the facts:" he used to say "All we want are the facts, ma'am" or "All we know are the facts, ma'am." The truncated version was invented by satirist Stan Freburg in a spoof called "Little Blue Riding Hood" recorded in 1953. The question of why he would say this primarily to women is left as a discussion for sociologists and historians interested in sexism of the 1950s.

## **Urban Myths**

The Urban Myths< <a href="http://www.urbanmyths.com/">http://www.urbanmyths.com/</a> > Web site differs from Snopes in appearance and focus, with bizarre photos and rude headlines such as "Americans Are Becoming Even Bigger Jerks Than Ever Before" and "How a Really Dumbass Publicity Stunt Broke Casey Afleck and May Still Destroy Joaquin Phoenix's Career." The contributors seem to be fascinated by bizarre and disgusting hoaxes and by true and horrifying bizarre stories. If you can stand being offended, the site may prove useful, but be prepared for insulting attacks on specific politicians using language suitable for a movie about teenaged prison inmates.

## **Vmyths**

For information debunking "computer security hysteria," the Vmyths< <a href="http://vmyths.com/">http://vmyths.com/</a> > site edited by Rob Rosenberger< <a href="http://vmyths.com/about/">http://vmyths.com/about/</a> > and George C. Smith, PhD, who have steadfastly countered advertising hyperbole and misinformation about antimalware products for more than two decades. They and their colleagues dissect news stories that misrepresent the role of malware and make unsubstantiated claims and predictions about cyber warfare and the end of the world through attacks on computers. These are intelligent contrarians who challenge accepted wisdom by demanding clear reasoning and factual support in all writing but especially in alarming writing.

### What about Politics?

All right then: Snopes and Urban Myths help us debunk fairy stories circulated by uncritical correspondents who forward anything scandalous or outrageous without bothering to check the facts and Vmyths fights hoaxes about malware. But where do we look for thorough, professional, unbiased analysis of recent statements from our politicians and political candidates?

#### **Politifacts**

In the United States (US), the PolitiFact< <a href="http://www.politifact.com/">http://www.politifact.com/</a> is the Snopes of politics. In her description of the origin and management of Politifact, Angie Drobnic Holan explains that "PolitiFact is a project of the St. Petersburg Times and its partner news organizations to help you find the truth in American politics." Strictly non-partisan, the 2009 Pulitzer Prize Winner<<a href="http://www.boston.com/news/politics/politicalintelligence/2009/04/politifact\_wins.html">http://www.boston.com/news/politics/politicalintelligence/2009/04/politifact\_wins.html</a> has expanded its resources by partnering with other news organizations across the US. The group has "received money from the Knight Foundation, Craigslist Charitable Fund, and the Collins Center for Public Policy."

Politifact published an amusing analysis< <a href="http://www.politifact.com/truth-o-meter/article/2011/nov/23/politifacts-guide-thanksgiving-dinner/">http://www.politifacts-guide-thanksgiving-dinner/</a> > of politically oriented chain letters circulating through e-mail in recent months. The story<
<a href="http://www.npr.org/2011/11/23/142670549/for-thanksgiving-debunk-your-familys-chain-emails">http://www.npr.org/2011/11/23/142670549/for-thanksgiving-debunk-your-familys-chain-emails</a> > was picked up by US National Public Radio on the Morning Edition show for Nov 23, 2011; the transcript includes a podcast of the six minute report.

### **FactCheck**

Another helpful resource for checking on political e-mail messages in the US is FactCheck<
http://www.factcheck.org/>, which is "A Project of the Annenberg Public Policy Center."
http://factcheck.org/about/> The organization describes itself as "a nonpartisan, nonprofit "consumer advocate" for voters that aims to reduce the level of deception and confusion in U.S. politics. We monitor the factual accuracy of what is said by major U.S. political players in the form of TV ads, debates, speeches, interviews and news releases. Our goal is to apply the best practices of both journalism and scholarship, and to increase public knowledge and understanding." It is funded through grants from foundations and public donations but states that "We do not seek and have never accepted, directly or indirectly, any funds from corporations, unions, partisan organizations or advocacy groups."

In the United Kingdom, The FactCheck Blog< http://blogs.channel4.com/factcheck/ > from

In the United Kingdom, The FactCheck Blog< <a href="http://blogs.channel4.com/factcheck/">http://blogs.channel4.com/factcheck/</a> > from Channel 4 News "goes behind the sp;in to dig out the truth and separate political fact from fiction;" it has archives dating back to June 2008. The "about" page<
a href="http://blogs.channel4.com/factcheck/welcome-to-the-new-factcheck-blog/18">http://blogs.channel4.com/factcheck/welcome-to-the-new-factcheck-blog/18</a> > states that the group has "won an award for statistical excellence in journalism, been cited in parliament and received a sack of email correspondence from readers, some very complimentary, some less so."

On the day I visited the FactCheck site (Nov 23. 2011), topics included

- How generous is Danny Alexander's pensions deal?
- Can Labour save the economy?
- Where are the real job opportunities?
- Are Britain's young people paying for the euro crisis?

- Who's lying about the border scandal?
- Is the Eurozone crisis strangling Britain's recovery?
- Are there any jobs out there?
- How much did James Murdoch know about phone hacking?
- Broken Britain and broken promises Clegg's riot payback collapses
- How dodgy stats could decide our children's future.

### **Advice for Family and Friends**

Finally, here is some of the text of a macro I have used since the late 1990s when responding to hoaxes that friends and relatives have forwarded to me:

#### \* \* \* A FRIENDLY MESSAGE ABOUT THE WARNING YOU JUST SENT ME \* \* \*

The warning you have forwarded is a hoax. The danger is imaginary and the problem is non-existent.

Security experts request that no one circulate unverified warnings of vague, alarming dangers.

Key indicators that a message is a hoax:

- Use of exclamation marks and in particular, multiple exclamation marks (no official warning uses them)!!!!!;
- Use of lots of UPPERCASE TEXT (typical of youngsters trying to EMPHASIZE points);
- Misspellings and bad grammar (typical of non-English speaking foreign phishers);
- No date of origination or expiration;
- Use of "yesterday," "last week," and "recently" with no way to tell what period these descriptions refer to;
- References to official-sounding sources or Web sites (e.g., MICROSOFT, CIAC, CERT) but no specific URL for details (nobody can legitimately cite <
   <a href="http://www.microsoft.com">http://www.microsoft.com</a> > as the source for a warning that hard disks will explode unless you give the sender your credit-card number);
- No valid digital signature from a known security organization;
- Requests to circulate widely (no such request is made in official documents).

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2011 M. E. Kabay. All rights reserved.

Permission is hereby granted to *InfoSec Reviews* to post this article on the *InfoSec Perception* Web site in accordance with the terms of the Agreement in force between *InfoSec Reviews* and M. E. Kabay.

### Free Slide Sets for Introduction to IA

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

I remember seeing university professors in my youth (1960s) using notes that were yellowed and curled: they had not been updated for years – sometimes decades. When I started teaching in the 1970s, I resolved explicitly never to use the previous year's notes without at least checking them for errors and updating them with current information. I still find mistakes and omissions in my work, but in general it's satisfying to provide students with each year's improved materials.

The IS340 "Introduction to Information Assurance" <

http://www.mekabay.com/courses/academic/norwich/is340/index.htm > course in the School of Business and Management
http://norwich.edu/academics/business/faculty.html > at Norwich University
http://www.norwich.edu > is a foundation course for the Bachelor of Science in Computer Security and Information Assurance (BSCSIA)

<a href="http://norwich.edu/academics/business/infoAssurance/index.html">http://norwich.edu/academics/business/infoAssurance/index.html</a> >. The course description<a href="http://www.mekabay.com/courses/academic/norwich/is340/is340\_course\_description.pdf">http://www.mekabay.com/courses/academic/norwich/is340/is340\_course\_description.pdf</a> > includes the following objectives:

By the end of this course, students will be able to discuss the following issues at a management level:

- Recognize, define and use the technical terminology of information assurance (IA).
- Name and define the fundamental concepts of IA.
- Describe models and key elements of information warfare.
- Recognize, name, define and discuss computer crime techniques; present countermeasures.
- Describe and discuss criminal-hacker subculture.
- Recognize, name, define, and discuss techniques of denial-of-service (DoS) attacks and countermeasures.
- Recognize, name, define, and discuss physical (facilities) security vulnerabilities and defenses.
- Recognize, name, define, and discuss identification and authentication techniques.
- Discuss specific security issues pertaining to voice and data networks.
- Recognize, name, define, and discuss fundamentals of firewalls and of intrusiondetection systems.
- Recognize, name, define, and discuss fundamentals of modern cryptography.
- Evaluate requirements and techniques for backing up, archiving, storing, managing, and destroying electronic records.

The course notes are available in PowerPoint (PPTX) and Adobe Portable Document Format (PDF) versions. A complete list<

http://www.mekabay.com/courses/academic/norwich/is340/is340\_lectures/is340\_filelist.pdf > showing the names and number of slides of all the files is available online. Each file is associated with one or two chapters in the textbook< http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529/ > we use in the course. The syllabus < http://www.mekabay.com/courses/academic/norwich/is340/is340\_syllabus.pdf > for the course

shows how the chapters are used in the two 1.5 hour classes throughout the semester.

Readers can take advantage of all the course materials freely for most educational purposes; for example, I hope the files will be useful for in-house training sessions and schools. The main restrictions on use are that

- No one should post any copy of the materials on a public Website (copies would make it difficult or impossible to maintain current versions for everyone);
- No one should sell the materials that I give away.

Full details of the copyright restrictions are available < <a href="http://www.mekabay.com/copyright.htm">http://www.mekabay.com/copyright.htm</a> >.

Speaking of copyright, most of the images in the files are licensed from iClipart < <a href="http://www.iclipart.com/index2.php">http://www.iclipart.com/index2.php</a> > and must not be extracted for use in new materials unless the user has a subscription to the service.

Finally, students and colleagues have commented on the bizarre images in some of the slides; they are included to amuse students and, in some cases, reawaken some exhausted military cadets who have to perform physical training at 05:00 before starting their day of study. Many of the images are visual puns.

I hope readers will find these resources helpful.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

Copyright © 2011 M. E. Kabay. All rights reserved.

Permission is hereby granted to *InfoSec Reviews* to post this article on the *InfoSec Perception* Web site in accordance with the terms of the Agreement in force between *InfoSec Reviews* and M. E. Kabay.

## **Checking for Data-Conversion Errors**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

In both the classic triad of information assurance (IA) and in the Parkerian Hexad< <a href="http://www.mekabay.com/overviews/hexad\_ppt.zip">http://www.mekabay.com/overviews/hexad\_ppt.zip</a>, integrity is a fundamental attribute of information that must be protected. Data integrity refers to the correctness of information; for example, integrity can refer to consistency with data's original and intended state.

Recently, a colleague and several of his research students ran into a problem when they tried to import data from a comma-delimited file (CSV<

http://creativyst.com/Doc/Articles/CSV/CSV01.htm >) into their version (2007<a href="http://office.microsoft.com/en-us/excel-help/up-to-speed-with-excel-2007-RZ010062103.aspx?CTT=1">http://office.microsoft.com/en-us/excel-help/up-to-speed-with-excel-2007-RZ010062103.aspx?CTT=1">http://office.microsoft.com/en-us/excel-help/up-to-speed-with-excel-2007-RZ010062103.aspx?CTT=1">http://office.microsoft.com/en-us/excel-help/up-to-speed-with-excel-2007-RZ010062103.aspx?CTT=1">http://office.microsoft.com/en-us/excel-help/up-to-speed-with-excel-2007-RZ010062103.aspx?CTT=1">http://office.microsoft.com/en-us/excel-help/up-to-speed-with-excel-2007-RZ010062103.aspx?CTT=1">http://office.microsoft.com/en-us/excel-help/up-to-speed-with-excel-2007-RZ010062103.aspx?CTT=1">http://office.microsoft.com/en-us/excel-help/up-to-speed-with-excel-2007-RZ010062103.aspx?CTT=1">http://office.microsoft.com/en-us/excel-help/up-to-speed-with-excel-2007-RZ010062103.aspx?CTT=1">http://office.microsoft.com/en-us/excel-help/up-to-speed-with-excel-2007-RZ010062103.aspx?CTT=1">http://office.microsoft.com/en-us/excel-help/up-to-speed-with-excel-2007-RZ010062103.aspx?CTT=1">http://office.microsoft.com/en-us/excel-help/up-to-speed-with-excel-2007-RZ010062103.aspx?CTT=1">http://office.microsoft.com/en-us/excel-help/up-to-speed-with-excel-2007-RZ010062103.aspx?CTT=1">http://office.microsoft.com/en-us/excel-help/up-to-speed-with-excel-2007-RZ010062103.aspx?CTT=1">http://office.microsoft.com/en-us/excel-help/up-to-speed-with-excel-2007-RZ010062103.aspx?CTT=1">http://office.microsoft.com/en-us/excel-help/up-to-speed-with-excel-2007-RZ010062103.aspx?CTT=1">http://office.microsoft.com/en-us/excel-help/up-to-speed-help/up-to-s

After deleting the tabs using the global replace function (CTL-H) to locate every 't character and replace it by nothing, the question arose of how to check the converted data against the original version that had contained the TAB characters. There was no point in applying the supposed correction if it caused discrepancies between the intended version of the data and the modified data.

separated by commas.

Sure enough, we immediately located some places where additional fixes would be required to make the data conform to the intended arrangement of rows and columns. After we found the discrepancies, it became clear that none of the students had ever thought about how to locate differences between two versions of their data.

There are several ways of checking for alterations of data in an Excel spreadsheet or in those that provide similar functions.

Figure 1. Using row and column totals for error-checking.

Original Table								
Alpha	Red	Orange	Yellow	Green	Totals			
Bravo	5	6	7	8	26			
Charlie	15	18	21	24	78			
Delta	45	54	63	72	234			
Echo	135	162	189	216	702			
Foxtrot	405	486	567	648	2106			
Totals	605	726	847	968				
Table with discrep	100	hlighted n						
- 11		11:11:1						
Table with discrep	oancies hig Red	hlighted n	nanually Yellow	Green	Totals			
Alpha	100	100		Green 8	Totals			
Alpha Bravo	Red	Orange	Yellow	//				
Alpha Bravo Charlie	Red 5	Orange 6	Yellow 7	8	26 78	Error must	be in this r	ow
	<b>Red</b> 5 15	Orange 6 18	Yellow 7 21	8 24	26 78	Error must	be in this r	ow
Alpha Bravo Charlie Delta	8ed 5 15 45	Orange 6 18 55	7 21 63	8 24 72	26 78 235	Error must	be in this r	ow
Alpha Bravo Charlie Delta Echo	5 15 45 135	Orange 6 18 55 165	7 21 63 189	8 24 72 216	26 78 235 705	Error must	be in this r	row

- One of the oldest methods for locating changes in tabular data is to compute totals for each row and for each column and look for differences in those totals. The row and the column where the totals differ from the originals pinpoint the difference in the cell contents. This method was something I used routinely back in the days of manual calculations, before spreadsheets were so refined that they became a kind of programming language. Figure 1 shows what this simple method looks like.
- Today, a simple and quick method is to use an IF statement to put an error indicator into a cell. As shown in Figure 2, one can simply define a function that sets a cell to something like "ERR" if the original cell value doesn't match the converted cell value.
- If for some reason you are not satisfied with simply printing an error message showing where a discrepancy lies, you can also use the conditional formatting options to colour a cell background as you see fit; in the example shown in Figure 3, all the correct cells are in green and discrepancies are flagged in red. The figure includes a screenshot of the conditional-formatting rules.

Figure 2. Using IF statements.

Alpha   Red   Orange   Yellow   Green   Total	Original Table					
Bravo		Red	Orange	Yellow	Green	Totals
Delta	Bravo		25.1	5111	100000000000000000000000000000000000000	26
Pecho   135   162   189   216   70	Charlie	15	18	21	24	78
Foxtrot         405         486         567         648         210           Totals         605         726         847         968           Totals           Alpha         Red         Orange         Yellow         Green         Total           Bravo         5         6         7         8         2           Charlie         15         18         21         24         7           Delta         45         55         63         72         23           echo         135         162         189         216         70           Foxtrot         405         486         567         648         210           Totals         605         727         847         968           Table using IF statements to highlight discrepancy           Alpha         Red         Orange         Yellow         Green         Total           Bravo         Charlie         ERR         ERI           Delta         ERR         ERI           echo         Foxtrot         ERR         ERR	Delta	45	54	63	72	234
Totals         605         726         847         968           Table with discrepancies highlighted manually         Alpha         Red         Orange         Yellow         Green         Total           Bravo         5         6         7         8         2           Charlie         15         18         21         24         7           Delta         45         55         63         72         23           echo         135         162         189         216         70           Foxtrot         405         486         567         648         210           Totals         605         727         847         968           Table using IF statements to highlight discrepancy           Alpha         Red         Orange         Yellow         Green         Total           Bravo         Charlie         ERR         ER         ER           Delta         ERR         ER         ER           Echo         Foxtrot         ER         ER         ER	echo	135	162	189	216	702
Table with discrepancies highlighted manually           Alpha         Red         Orange         Yellow         Green         Total           Bravo         5         6         7         8         2           Charlie         15         18         21         24         7           Delta         45         55         63         72         23           echo         135         162         189         216         70           Foxtrot         405         486         567         648         210           Totals         605         727         847         968           Table using IF statements to highlight discrepancy           Alpha         Red         Orange         Yellow         Green         Total           Bravo         Charlie         ERR         ER         ER           Delta         ERR         ER         ER           Echo         Foxtrot         ER         ER         ER	Foxtrot	405	486	567	648	2106
Bravo	Totals	605	726	847	968	
Alpha         Red         Orange         Yellow         Green         Total           Bravo         5         6         7         8         2           Charlie         15         18         21         24         7           Delta         45         55         63         72         23           echo         135         162         189         216         70           Foxtrot         405         486         567         648         210           Totals         605         727         847         968           Table using IF statements to highlight discrepancy           Alpha         Red         Orange         Yellow         Green         Total           Bravo         Charlie         ERR         ER         ER           Delta         ERR         ER         ER           Foxtrot         Foxtrot         Foxtrot         Foxtrot         Foxtrot         Foxtrot	Table with discrep	ancies hid	ahlighted m	nanually		
Charlie         15         18         21         24         7.7           Delta         45         55         63         72         23           echo         135         162         189         216         70           Foxtrot         405         486         567         648         210           Totals         605         727         847         968           Table using IF statements to highlight discrepancy           Alpha         Red         Orange         Yellow         Green         Total           Bravo         Charlie         ERR         ERI           Delta         ERR         ERI           echo         Foxtrot         ERI		107	25 75		Green	Totals
Delta         45         55         63         72         23           echo         135         162         189         216         70           Foxtrot         405         486         567         648         210           Totals         605         727         847         968           Table using IF statements to highlight discrepancy           Alpha         Red         Orange         Yellow         Green         Total           Bravo         Charlie         ERR         ERI           Delta         ERR         ERI           echo         Foxtrot         ERI	Bravo	5	6	7	8	26
Page 2016   Page	Charlie	15	18	21	24	78
Foxtrot 405 486 567 648 210  Totals 605 727 847 968  Table using IF statements to highlight discrepancy  Alpha Red Orange Yellow Green Total  Bravo Charlie Delta ERR ERR ERR FOXTrot	Delta	45	55	63	72	235
Totals 605 727 847 968  Table using IF statements to highlight discrepancy  Alpha Red Orange Yellow Green Total  Bravo  Charlie  Delta ERR ERI  echo  Foxtrot	echo	135	162	189	216	702
Table using IF statements to highlight discrepancy  Alpha Red Orange Yellow Green Total  Bravo  Charlie  Delta ERR ERI  echo  Foxtrot	Foxtrot	405	486	567	648	2106
Alpha Red Orange Yellow Green Total Bravo Charlie Delta ERR ERI echo Foxtrot	Totals	605	727	847	968	
Bravo Charlie Delta ERR ERI echo Foxtrot	Table using IF sta	tements to	o highlight	discrepanc	y	
Charlie  Delta ERR ERI echo  Foxtrot	Alpha	Red	Orange	Yellow	Green	Totals
Delta ERR ERI echo Foxtrot	Bravo					
echo Foxtrot	Charlie					
Foxtrot	Delta		ERR			ERR
A CONTROL OF THE CONT	echo					
Totals ERR	Foxtrot					
	Totals		ERR			
			_cell=new ,"","ERR")	_cell,"",ERF	₹")	

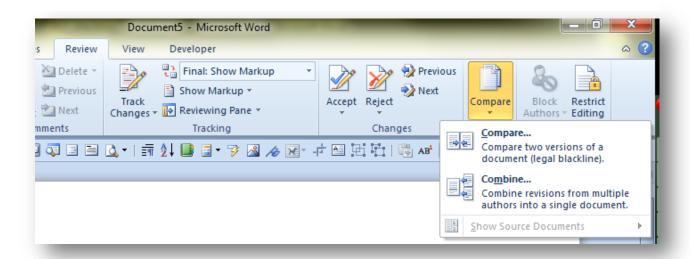
Figure 3. Using conditional formatting.

Original Table							
Alpha	Red	Orange	Yellow	Green	Totals		
Bravo	5	6	7	8	26		
Charlie	15	18	21	24	78		
Delta	45	54	63	72	234		
Echo	135	162	189	216	702		
Foxtrot	405	486	567	648	2106		
Totals	605	726	847	968			
Table with discr	100			Creen	Tatala		
Alpha	Red	Orange	Yellow	Green	Totals		
Bravo	5	6	7	8	26		
Charlie	15	18	21	24	78		
Delta	45	55	63	72	235		
Echo	135	162	189	216	702		
Foxtrot	405	486	567	648	2106		
Totals	605	727	847	968			
Table using IF st	tatements p	lus conditi	onal format	ttina to hia	hliaht discrepa	incv	
Alpha	Red	Orange	Yellow	Green			
Bravo	OK	ОК	ОК	ОК			
Charlie	ОК	ОК	OK	ОК			
Delta	ОК	ERR	ОК	ОК			
Echo	ОК	ОК	ОК	OK			
Foxtrot	ОК	ок	ОК	ок			
Formula:	if/ autain al		!! !!! 505	201			
Example:	=if(original =IF(B5=B14		_cell, ,EKI	( )			
example.	-17(03-014	, , ENN )					
Conditional rule	es:						
C	Min - Dulan	Managara					? X
Conditional Form	- 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1	ivianager					
Show formatting	rules for:	irrent Selectio	n .				
New Rule	. <u>Bedit</u>	Rule	X Delete Ru	ıle 🔺	•		
Rule (applied in	order shown)	Format		Applies to			Stop If True 🔺
Cell Value =	= "ERR"	AaBt	IGCYy Zz	=\$B\$23:\$I	E\$27		
Cell Value =	= "OK"	AaBb	CcYyZz	=\$B\$23:\$I	E\$27		
500000000000000000000000000000000000000							
							+

What if you have to compare other data files such as TXT plain-ASCII? A trick you can use is to arrange the files to be exactly the same in font, point size and position on the screen (e.g., filling an entire screen). In Windows, you can press Alt-Tab repeatedly to switch between the files. Any difference between the two will show up as a moving or changing element as you flash back and forth between the files. However, this method does depend on the viewer's attention for its effectiveness; it's also difficult to manage for large files that take more than one screen to visualize. For rows or columns in the thousands, it's impractical.

Another approach is to use WORD's file comparison feature. In Word 2007 and Word 2010, the **Review** tab has a **Compare** function that provides the option to "**Compare...** Compare two versions of a document (legal blackline)." Figure 4 shows the dialog to initiate a comparison. Everything that differs between the two documents will be highlighted in colour.

Figure 4. Using WORD comparison function.



If anyone wants to see the Excel 2010 spreadsheet used to create Figures 1 through 3, it is available here < <a href="http://www.mekabay.com/perception/011\_checking\_for\_data-conversion\_errors.xlsx">http://www.mekabay.com/perception/011\_checking\_for\_data-conversion\_errors.xlsx</a>>.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

Copyright © 2011 M. E. Kabay. All rights reserved.

Permission is hereby granted to *InfoSec Reviews* to post this article on the *InfoSec Perception* Web site in accordance with the terms of the Agreement in force between *InfoSec Reviews* and M. E. Kabay.

# **Macintosh Malware Erupts**

by Jeremy Legendre
BSCSIA Student, Norwich University
&

M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

MK writes: Norwich University student Jeremy Legendre sent me an interesting essay which prompted a close collaboration between the two of us on this article.

\* \* \*

### **History**

Sophos antimalware expert Graham Cluley< <a href="http://www.linkedin.com/in/grahamcluley">http://www.linkedin.com/in/grahamcluley</a>>, who has a long and distinguished career in the field, has written a summary of malicious software affecting Macintosh computers.[1] In comparison to the history of Windows malware,[2] Macintosh systems have been far less susceptible to malware than Windows systems. For example, in 2005, Mark H. Anbinder and colleagues published a review of Macintosh computer malware in which (in the version available through the EBSCO library database provided by Norwich University) *Macworld* editors started the review with this note: "Most Mac users gaze on smugly as reports of each new Windows security crisis break. And they have good reason: At press time, research from Sophos (a maker of antivirus software) showed that 68 viruses have affected the Mac while 97,467 have affected Windows. Of those 68, most are a decade old or older and don't directly affect OS X."

Despite the disparity in the number of viruses affecting Windows and Macintosh systems, Anbinder *et al.* challenged the belief that "Mac users don't need to worry about viruses." The authors warned readers that "We've enjoyed a long, glorious stretch without serious malware affecting our platform. But that doesn't mean we can afford to let down our collective guard. If there is a virus attack, those of us who have good, up-to-date antivirus software installed will have the best odds of escaping unscathed." They urged Mac users to keep updated antimalware tools – and back in 2005, it was reasonable to suggest, "Weekly updates should be adequate for most users, but if your computing involves accessing lots of files from lots of sources—whether via e-mail, file servers, or Web downloads—then daily updates might be a better idea."

## Changes

However, malware specifically designed for Mac is on the rise. Cluley's historical summary shows progressively more and more serious malware in 2009, 2010 and 2011. Apple products have been increasing their market share for laptops and workstations but especially for tablets and phones. Writing in the *Wall Street* Journal, Nick Winfield pointed out that "Some research firms have even started to look at tablets as part of the PC market when determining market share, which significantly changes Apple's position. Canalys Ltd., for example, now calls Apple the second-largest PC vendor, after Hewlett Packard Co. Adding in iPads as well as Macs –

which only accounted for about 5% of global shipments – the firm estimates that Apple accounted for 13.6% in world-wide PC shipments in the second quarter, up from 8.2% a year earlier, and just a bit behind H-P's 15.7% share."[4]

It seems reasonable to predict that black hats would to follow the trend in market share, and recently, evidence has surfaced of new Macintosh operating system malware. Ed Bott reported on an interview with an anonymous AppleCare support representative who told him in May 2011 about increasing calls to AppleCare support because of malware.[5] Apparently the "Mac Defender"[6] virus was causing four to five times as many calls as usual.

Jeremy personally reverse-engineered and analyzed Mac Defender to see what the fuss was all about. As it turns out, this piece of malware is very simple and could be easily stopped by Apple with a service package or update. If this simple little program is causing such an increase in AppleCare calls, what is going to happen when more advanced malware comes out?

On May 2<sup>nd</sup>, 2011, a Danish security company named CSIS Security Group announced something that has never been seen before: the first do-it-yourself crimeware kit for the Mac.[7] It has been put up for sale on a few underground forums. Not all the details on what the crimeware kit can do have been released yet, but Brian Krebs interviewed the author of the malware: "The seller of this crimeware kit claims his product supports form-grabbing in Firefox and Chrome, and says he plans to develop a Linux version and one for the iPad in the months ahead. The price? \$1,000, with payment accepted only through virtual currencies Liberty Reserve or WebMoney."[8] Krebs includes a link to a YouTube video showing details of the crimeware's user interface.

Apple posted instructions on "How to avoid or remove Mac Defender malware" in June 2011.[9]

## **Concluding Remarks from Jeremy**

One of the reasons Mac OS X is perceived as superior to Windows is because of its appearance of having integrated security; for example, requiring user credentials before running any system changing software or claiming that "With virtually no effort on your part, OS X defends against viruses and other malicious applications, or malware. For example, it thwarts hackers through a technique called "sandboxing" — restricting what actions programs can perform on your Mac, what files they can access, and what other programs they can launch."[10]

Although the design may be sound, the operating system does *not* prevent people from being swayed into *thinking* that the malicious software they are downloading is safe. Although a user cannot install a program on a Mac without user permission, an unsuspecting user may easily allow malware to run. From this point of view, Mac OS X is *not* fundamentally safer than Windows or Linux. I do not say this as someone who is anti-Mac: I use my Macbook Pro every day and I love it, but I am still cautious about what I install on it. But without adapting to the changing threat picture, Apple will be in the same position of malware vulnerability that Microsoft has reached.

So, in conclusion, Macs are starting to become more popular and a wider range of people are using their systems. Apple will have to concentrate more on security and vulnerability within their operating system. They are going to have to have more security updates and patches and may have to stop their "It doesn't get PC viruses" ad campaign from which I quoted in the first

paragraph of these concluding remarks.

Although Apple may not like having to admit that their systems are susceptible to viruses, awareness of the changing malware situation gives them a chance to get ahead of the curve by strengthening the operating system and find additional ways to prevent further malware attacks.

#### **Notes**

[1] (Cluley 2011) (Leonhard 2011) [2] [3] (Anbinder, et al. 2005) [4] (Wingfield 2011) [5] (Bott, An AppleCare support rep talks: Mac malware is "getting worse" 2011) (Bott, What a Mac malware attack looks like 2011) [6] [7] (Kruse 2011) (Krebs 2011) [8] [9] (Apple, How to avoid... 2011)

#### **Works Cited**

[10]

Anbinder, Mark H, Jeff Carlson, Glenn Fleishman, Jeffery Battersby, and Kirk McElhearn. "Mac Security: Fact and Fiction." *Macworld* 22, no. 3 (2005-02-18): 54-64.

http://www.macworld.com/article/42964/2005/02/macsecuritymain.html (accessed 2011-12-07).

Apple. How to avoid or remove Mac Defender malware. 2011-06-08.

http://support.apple.com/kb/HT4650 (accessed 2011-11-22).

(Apple, Why you'll love... 2011)

—. "Why you'll love a Mac -- It doesn't get PC viruses." Apple Inc. 2011.

http://www.apple.com/why-mac/better-os/#viruses (accessed 2011-12-07).

Bott, Ed. An AppleCare support rep talks: Mac malware is "getting worse". 2011-05-11.

http://www.zdnet.com/blog/bott/an-applecare-support-rep-talks-mac-malware-is-getting-worse/3342 (accessed 2011-11-21).

—. What a Mac malware attack looks like. 2011-05-06. <a href="http://www.zdnet.com/blog/bott/what-a-mac-malware-attack-looks-like/3269?tag=content;siu-container">http://www.zdnet.com/blog/bott/what-a-mac-malware-attack-looks-like/3269?tag=content;siu-container</a> (accessed 2011-11-21).

Cluley, Graham. The short history of Mac malware: 1982 - 2011. 2011-10-03.

http://nakedsecurity.sophos.com/2011/10/03/mac-malware-history/ (accessed 2011-11-21).

Krebs, Brian. 'Weyland-Yutani' Crime Kit Targets Macs for Bots. 2011-05-11.

http://krebsonsecurity.com/tag/weyland-yutani-bot/ (accessed 2011-11-21).

Kruse, Peter. Crimekit for MacOSX launched. 2011-05-02.

http://www.csis.dk/en/csis/blog/3195/ (accessed 2011-11-21).

Leonhard, Woody. 20 years of innovative Windows malware -- Ingenuity to nefarious ends: The evolution of groundbreaking Windows malware sheds light on what's to come. 2011-02-28. <a href="http://www.infoworld.com/d/security/20-years-innovative-windows-malware-021">http://www.infoworld.com/d/security/20-years-innovative-windows-malware-021</a> (accessed 2011-11-21).

Wingfield, Nick. "Microsoft Faces the Post-PC World -- Now 25 Years Old, Windows Sales Slow as iPad Gains; Lowest Market Share in Two Decades -- 82%." *The Wall Street Journal*, 2011-08-15: B1.

http://online.wsj.com/article/SB10001424053111903885604576486343139938136.html (Subscription required; accessed through Norwich University Kreitzberg Library databases 2011-12-07).

Jeremy Legendre has been programming since he was 14; he is now is one of our most gifted freshmen in the BSCSIA program at Norwich University. He is currently collaborating with one of our professors on a textbook for an upper-level malware forensics course.

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

Copyright © 2011 Jeremy Legendre & M. E. Kabay. All rights reserved.

Permission is hereby granted to *InfoSec Reviews* to post this article on the *InfoSec Perception* Web site in accordance with the terms of the Agreement in force between *InfoSec Reviews* and M. E. Kabay.

# **Coping with a Compromised E-mail Account**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

From: Colleague
To: Mich Kabay

RE: Compromised e-mail account

Dear Mich,

Someone has stolen one of my e-mails (not NU), and is using it to ask for money by sending messages to my entire contact list. What can be done apart from changing my password?

\* \* \*

#### Dear Colleague,

I discussed your situation with a colleague who has more experience responding to cybercrimes. The criminals *may* be

- using your e-mail account OR
- using one with a similar e-mail identification OR
- forging the e-mail headers to make it look as if they have control of your account.

Without access to the actual messages your friends received (including the usually hidden header fields), we cannot tell which technique(s) the criminals are using. If they are using a different account or forging the headers, they presumably have your distribution list to be able to reach your correspondents.

#### Our recommendations are as follows:

- 1) Change the password on your e-mail immediately to a difficult-to-guess form; e.g., uja\*RODIN\_39. Using random syllables (consonant-vowel) helps you remember the password. Record it in a safe place so you can get the remaining e-mails you will need.
- 2) Establish a new e-mail account with a name noticeably different from the one you have used in the compromised account; e.g., if you were, say, < colleague@gmail.com >, perhaps the new account would be < nucolleague@gmail.com >. If there are security questions beyond the password, choose questions you have not used before; e.g., if your old e-mail account had a question about your city of birth, don't use that particular question for the new account.
- 3) Be sure that you can transfer your contact list to the new e-mail account; if there is no provision from the e-mail supplier, then be sure that you have an independent backup of the list such as a file. Normally, you can store all your addresses in your OUTLOOK contact list that is part of the University's standard software on our laptop computers.

- 4) Using the *old* (possibly compromised) account, immediately send an e-mail message to everyone on your contact list telling them that
  - a) you are OK and they should ignore messages claiming that you are in trouble and need money;
  - b) you are shutting down your current e-mail account because it is no longer trustworthy;
  - c) you will be using the new account called < \_\_\_\_\_ > (fill in new address);
  - d) if they can, they should add the old address to their JUNK filter.

Put some details into your signature block so people can have confidence that it's really you sending the message; e.g., include info such as your professorial title or your phone number.

- 5) Contact or log on to the account-management pages for every mailing-list you subscribe to or association you belong to and change your e-mail address to the new one using their change-of-address procedures. Occasionally, you may need to do this using your *old* (compromised) account because some mailing lists send confirmation of a proposed e-mail change to the *original* (old) e-mail address for verification. That approach interferes with the ability of criminals to redirect your correspondence without your permission.
- 6) Shut down the compromised account. Use the procedures available from your e-mail supplier generally available through their HELP feature.
- 7) More generally, be absolutely sure that you never use a password for more than one account. If there are *any* accounts which use the same password as the compromised account, you *must* change their passwords at once.
- 8) You may store your passwords securely in OUTLOOK on your computer by creating a new contact card and checking the "Private" button (looks like a padlock) in the CONTACT sheet. You should create a separate contact card for each Website or other password-protected function.
- Do not use the Internet Explorer "remember password" function. There is no security to prevent someone who has access to your computer from logging in to password-protected. Modern browsers offer a "password safe" feature that will remember the password for each Website but impose a master password. If you use Internet Explorer as your browser, download and install Bruce Schneier's "Password Safe" software which is safe, secure and free: < http://passwordsafe.sourceforge.net/ >. It will impose a master password on the "safe" so that only you will be able to use your other passwords on Websites. Effectively, you will have only one password to remember even though you may have hundreds of different, complicated ones. My passwords (but not the master password) look like this: 8\*4Jur\_hvn(\_gaM. Because the computer password safe remembers them, they are all very difficult for a criminal to guess ("break").

#### Good luck!

For further reading on this subject with additional practical suggestions, see the following articles.

- Boatman, K. (2007). "How to Recover When Your Email Account Is Hacked." *Earthlink Security Center* < <a href="http://www.earthlinksecurity.com/articles/email\_hacked/index.html">http://www.earthlinksecurity.com/articles/email\_hacked/index.html</a> >.
- Chase, J. (2011). "Hacked and Hijacked: What to Do if Your E-mail Account Gets Compromised." *Switched* < <a href="http://www.switched.com/2011/02/24/what-to-do-email-account-hacked/">http://www.switched.com/2011/02/24/what-to-do-email-account-hacked/</a> > (2011-02-24).
- "Security, Doctor" (2011). "What to Do When Your Email Account Has Been Compromised." Zone-Alarm by Check Point < <a href="http://blog.zonealarm.com/2010/06/what-to-do-when-your-email-account-has-been-compromised.html">http://blog.zonealarm.com/2010/06/what-to-do-when-your-email-account-has-been-compromised.html</a> > (2011-06-10).

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

Copyright © 2011 M. E. Kabay. All rights reserved.

Permission is hereby granted to *InfoSec Reviews* to post this article on the *InfoSec Perception* Web site in accordance with the terms of the Agreement in force between *InfoSec Reviews* and M. E. Kabay.

# **Changing Conceptions of Privacy**

by Maria Dailey & M. E. Kabay, PhD, CISSP-ISSMP School of Business & Management Norwich University, Northfield VT

Maria Dailey is a senior in the Bachelor of Science in Computer Security and Information Assurance (BSCSIA) in the School of Business at Norwich University. She recently submitted an interesting essay in the IS455 Strategic Applications of Information Technology<
<a href="http://www.mekabay.com/courses/academic/norwich/is455/index.htm">http://www.mekabay.com/courses/academic/norwich/is455/index.htm</a> course, and I suggested to her that we work together to edit and expand it for publication. The following is the result of a close collaboration between us.

\* \* \*

#### **NTHNTF?**

Privacy opponents feel that there is no need for privacy. If there is nothing to hide, there exists no real excuse to hide information. That belief is often described as the nothing-to-hide-nothing-to-fear (NTHNTF) position. In an extreme statement of this position, former *News of the World* deputy features editor Paul McMullan, speaking before the Leveson inquiry[1], said,

"In 21 years of invading people's privacy I've never actually come across anyone who's been doing any good. Privacy is the space bad people need to do bad things in. Privacy is for paedos. If there is a privacy law your secrets are going to be much more valuable than they were before."[2]

Those opposed to NTHNTF belief argue that certain information taken out of context can result in undeserved consequences to innocent citizens. "Privacy protects us from being misdefined and judged out of context in a world...in which information can easily be confused with knowledge."[3]

The *Privacy, Identity & Consent Blog*[4] author, Toby Stevens,[5] summarizes current developments in privacy law and policy; in one posting at the end of 2010, he articulates his concerns about the effects of the Internet on privacy:

"In 1890, Samuel Warren and Louis Brandeis famously described privacy as "the right to be let alone." For over a century since then, society has developed legal, technical and social frameworks that protected a concept of alone-ness, of isolation, of keeping others away from the individual and information about that individual. Our concept of privacy has become one of 'urban anonymity:' we believe we have some degree of anonymity when we are in public, since if nobody knows who we are, then our actions cannot have consequences since we can't be identified.

But ... the emergence of the Internet has stood that idea on its head in the past ten years. The explosion of data, of access to that data, of tools to search, filter, analyse, interrogate, present and disseminate that data, placed in the hands of government, companies and individuals have stripped away that veneer of anonymity and created a dystopia in which our privacy is fading, not because of our failure to control privacy, but because privacy itself has changed, and the old controls are no longer able to contain or to manage the ways in which we share information with others....

Privacy is no longer about keeping our personal information secret, but is instead about controlling how it is used. And unless we can enforce that control, the only possible outcome for our society is total transparency: a world in which nobody has any secrets at all, and individuals have no meaningful control over how those secrets are used. Nothing is ignored, nothing is forgotten, nothing is forgiven..."[6]

#### **Radically Increased Access**

One of the developing features of information technology is how much information one can find about another person. White Pages on Yellowpages.com permits any user to look up the current telephone and address of anyone within the United States, as long as the individual searched for is listed.[7] Although this is a digital version of a paper book most people receive at home, it provides a wider pool of both searchers and targets, no longer limiting then to a common area – or increasing the common area to the entire nation.

Other Websites, such as MyLife.com, provide more detailed information on specific individuals to anyone who has signed up and chosen an inexpensive membership. Anyone can join and acquire as much information as he or she desires. MyLife "helps you find people from anytime in your life, no matter where they are," and aims to "provide the most comprehensive people search service." MyLife provides information on over 750 million people by collecting publicly available information, and has a feature enabling anyone with a paid account to see who is searching for him or her. [8] This "publicly available information" is extensive, and reaches further when individuals do not protect information they wish to remain exclusively available to certain people.

Electronic searches may increase the susceptibility to crime. In a recent summary, Mark Jenkins of Channel 13 News in Orlando, Florida warned that social-media users should not post detailed information about their vacation plans: "...[T]hanks to social networks, criminals can tell the moment you leave your home and how long you're gone. They'd have easy access to your vacant home." He quoted a police officer with specific advice:

Corporal Marcus Camacho with the Orange County Sheriff's Office said it's a major travel mistake. "[With] Smart phones, today, you can update your location so anybody could know where you're at, at any time," Camacho said. "What they don't realize is people are seeing that. Especially if you have a public view on your social networking site that everybody can see that."[9]

Google Earth can provide photographs of many addresses from street level.[10] Shortly after it was introduced, there was a flurry of concerns about the effects of street-level, detailed photographs on privacy; for example, *TIME Magazine* writer S. James Snyder wrote in 2007,

"Google's new "Street View" has sent techies scrambling to browse through the miles and miles of street-level photos now available through Google Maps. But while such blogs as BoingBoing.net and Mashable.com have made something of a joke out of the many humorous (a man apparently caught mid-sneeze), bizarre (the ghost of E.T.?) and lewd (a woman's underwear poking out of her low-riding jeans) images captured by the web giant, privacy concerns have led many watchdog groups to quickly retort that Street View is no laughing matter."[11]

Google responded quickly, publishing a privacy page about street-level *Google earth*. Among the privacy protections outlined are

- Photographs are from public access only;
- The images can be several months old;
- Individuals and license plates are automatically blurred;
- Anyone can request additional blurring of details or removal of images containing objectionable material such as nudity or violence.

#### **Concluding Remarks**

Changing communications technology has already begun to change the nature of privacy. Users of the Web and related services should think about the implications of public disclosure of information and filter their postings with what may become *common sense* in a generation or so but is to date definitely still *uncommon* sense.

In the next posting, Maria and Mich will discuss privacy implications of recent controversies over social networking sites and privacy.

#### References

- [1] Guardian 2011
- [2] Halliday and O'Carroll 2011
- [3] Privacy Rights Clearinghouse 2011
- [4] Stevens, Privacy, Identity & Consent: The Data Trust Blog 2011
- [5] Enterprise Privacy Group 2011
- [6] Stevens, Private Lives in a Database World 2010
- [7] AT&T 2011
- [8] MyLife.com Inc 2011
- [9] Jenkins 2011
- [10] Google 2011
- [11] Snyder 2007

#### **Works Cited**

- AT&T. White Pages. 2011. http://www.yellowpages.com/whitepages (accessed 11 24, 2011). Enterprise Privacy Group. "Company Profile: The EPG Team." Enterprise Privacy Group. 2011. http://www.privacygroup.org/content/view/18/23/ (accessed 12 24, 2011).
- Google. Google earth. 2011. http://www.google.com/earth/index.html (accessed 12 24, 2011).
- Guardian. *Leveson inquiry*. 12 2011. <a href="http://www.guardian.co.uk/media/leveson-inquiry">http://www.guardian.co.uk/media/leveson-inquiry</a> (accessed 12 24, 2011).
- Halliday, Josh, and Lisa O'Carroll. *Rebekah Brooks and Andy Coulson are 'scum of journalism'*, *Leveson told.* 29 11 2011. <a href="http://www.guardian.co.uk/media/2011/nov/29/rebekah-brooks-andy-coulson-leveson-inquiry">http://www.guardian.co.uk/media/2011/nov/29/rebekah-brooks-andy-coulson-leveson-inquiry</a> (accessed 12 24, 2011).
- Jenkins, Mark. "You may be leading burglars to your house with online posts." *Central Florida News 13*. 23 12 2011. <a href="http://www.cfnews13.com/article/news/2011/december/360770/You-may-be-leading-burglars-to-your-house-with-online-posts">http://www.article/news/2011/december/360770/You-may-be-leading-burglars-to-your-house-with-online-posts</a> (accessed 12 23, 2011). MyLife.com Inc. "About US." *MyLife*. 2011. <a href="http://www.mylife.com/aboutUs.pub">http://www.mylife.com/aboutUs.pub</a> (accessed 12 24, 2011).
- Privacy Rights Clearinghouse. *Privacy Today: A Review of Current Issues*. 1 March 2011. https://www.privacyrights.org/ar/Privacy-IssuesList.htm#dataprofiling (accessed 11 30, 2011).
- Snyder, S. James. "Google Maps: An Invasion of Privacy?" *TIME Business*. 12 06 2007. <a href="http://www.time.com/time/business/article/0,8599,1631957,00.html">http://www.time.com/time/business/article/0,8599,1631957,00.html</a> (accessed 12 24, 2011).
- Stevens, Toby. *Privacy, Identity & Consent: The Data Trust Blog.* 24 08 2011. http://www.computerweekly.com/blogs/the-data-trust-blog/ (accessed 12 23, 2011).
- —. "Private Lives in a Database World." *Privacy, Identity & Consent: The Data Trust Blog.* 07 12 2010. <a href="http://www.computerweekly.com/blogs/the-data-trust-blog/2010/12/private-lives-in-a-database-wo.html">http://www.computerweekly.com/blogs/the-data-trust-blog/2010/12/private-lives-in-a-database-wo.html</a> (accessed 12 24, 2011).

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2012 Maria Dailey & M. E. Kabay. All rights reserved.

# **Social Networks and Privacy**

by Maria Dailey & M. E. Kabay, PhD, CISSP-ISSMP School of Business & Management Norwich University, Northfield VT

Maria Dailey is a senior in the Bachelor of Science in Computer Security and Information Assurance (BSCSIA) in the School of Business at Norwich University. She recently submitted an interesting essay in the IS455 Strategic Applications of Information Technology<
<a href="http://www.mekabay.com/courses/academic/norwich/is455/index.htm">http://www.mekabay.com/courses/academic/norwich/is455/index.htm</a> > course, and I suggested to her that we work together to edit and expand it for publication. The following is the result of a close collaboration between us and continues last week's column about changing conceptions of privacy.

\* \* \*

#### **Social Network Sites and Privacy**

Harvey Jones and José Hiram Soltren published an interesting early study of privacy practices on Facebook in 2005.[1] They wrote in their abstract, "Privacy on Facebook is undermined by three principal factors: users disclose too much, Facebook does not take adequate steps to protect user privacy, and third parties are actively seeking out end-user information using Facebook." Key findings of the study (page 13) include the following (quoting, with bullets added):

- Users put real time and effort into their profiles.
- Students tend to join as soon as possible, often before arriving on campus.
- Users share lots of information but do not guard it.
- Users give imperfect explicit consent to the distribution and sharing of their information.
- Privacy concerns differ across genders.

For adolescents regularly using social networking sites (SNSs), reactions to their postings are emotionally significant. In a study of 881 teenagers in the Netherlands by Valkenburg, Peter and Schouten, the authors explored "...the consequences of friend networking sites (e.g., Friendster, MySpace) for adolescents' self-esteem and well-being." The young people spent an average of half an hour online every few days; the most important factor correlated with the participants' self-esteem was the tone of the comments on their postings. "Positive feedback enhanced adolescents' self-esteem, and negative feedback decreased their self-esteem. Most adolescents (78%) always or predominantly received positive feedback on their profiles. For these adolescents, the use of friend networking sites may be an effective vehicle for enhancing their self-esteem."[2]

On the other hand, sometimes users of SNSs may go too far in posting intimate details of their lives. Linda Roeder summarized some of the issues[3] to consider before posting information online in personal Web pages (or SNSs), including the following:

- How much identifying detail (full name, address, phone number...) should parents post about their children?
- How much intimate detail should users post about their inner thoughts and feelings?
- Should you avoid hyperlinks to your personal Web pages to prevent web-crawlers from indexing material you want to keep to a limited circle of friends?

The *Who's Watching* Website warns, "Sharing too much information on social networking sites can be problematic in two ways: first, it can reveal something about you that you'd rather your current or future employer or school administrator not know, and second, it can put your personal safety at risk."[4]

SNSs such as Facebook, Twitter, and MySpace all have privacy features that users can implement to protect their information against indiscriminate access. In the United States, these sites must meet requirements set by the Federal Trade Commission (FTC). However, SNSs have not always abided by regulations.

In December 2009, the Electronic Privacy Information Center (EPIC) and nine other privacy organizations filed a complaint with the FTC alleging privacy violations by Facebook. The introduction included this description:

"This complaint concerns material changes to privacy settings made by Facebook, the largest social network service in the United States, which adversely impact users of the Facebook service. Facebook's changes to users' privacy settings disclose personal information to the public that was previously restricted. Facebook's changes to users' privacy settings also disclose personal information to third parties that was previously not available. These changes violate user expectations, diminish user privacy, and contradict Facebook's own representations. These business practices are Unfair and Deceptive Trade Practices...."[5]

FTC Commissioners found that Facebook misled members into believing that clicking on strict privacy settings in the "Central Privacy Page" and the "Profile Privacy Page" would allow them to close access to their information for everyone but "friends" or "friends of friends" if they so wished. However, wrote the Commissioners,

"None of the pages described in Paragraphs 10-13 have disclosed that a user's choice to restrict profile information to 'Only Friends' or 'Friends of Friends' would be ineffective as to certain third parties. Despite this fact, in many instances, Facebook has made profile information that a user chose to restrict to 'Only Friends' or 'Friends of Friends' accessible to any Platform Applications that the user's Friends have used (hereinafter 'Friends' Apps'). Information shared with such Friends' Apps has included, among other things, a user's birthday, hometown, activities, interests, status updates, marital status, education (e.g., schools attended), and place of employment, photos, and videos."[6]

In addition, the Commissioner found that the privacy provisions against applications were misleadingly labelled (quoting directly):

"However, in many instances, the links to 'Applications,' 'Apps,' or 'Applications and Websites' have failed to disclose that a user's choices made through Profile Privacy Settings have been ineffective against Friends' Apps. For example, the language alongside the Applications link, depicted in Paragraph 10, has stated, '[c]ontrol what information is available to applications you use on Facebook.' .... Thus, users who did not themselves use applications would have had no reason to click on this link, and would have concluded that their choices to restrict profile information through their Profile Privacy Settings were complete and effective."[6]

The proposed settlement [7] between the FTC and Facebook was summarized by the EPIC as follows:

"Specifically, under the proposed settlement, Facebook is:

- barred from making misrepresentations about the privacy or security of consumers' personal information;
- required to obtain consumers' affirmative express consent before enacting changes that override their privacy preferences;
- required to prevent anyone from accessing a user's material more than 30 days after the user has deleted his or her account;
- required to establish and maintain a comprehensive privacy program
  designed to address privacy risks associated with the development and
  management of new and existing products and services, and to protect the
  privacy and confidentiality of consumers' information; and
- required, within 180 days, and every two years after that for the next 20 years, to obtain independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order, and to ensure that the privacy of consumers' information is protected."[8]

#### Lessons

Users of Internet-mediated information-gathering services must remain on guard to prevent abuse of their privacy. Users should monitor changes in terms of service for Websites – including especially SNSs.

Corporate officers may be attracted to increasing revenue through deceptive practices; government and law enforcement officials may be interested in snooping illegally into the behaviour of individuals. Knowing that the public is keeping a watchful eye on their behaviour may serve to keep them honest.

Supporting tracking of privacy issues through organizations such as EPIC< <a href="https://npo.networkforgood.org/Donate/Donate.aspx?npoSubscriptionId=8252">https://npo.networkforgood.org/Donate/Donate.aspx?npoSubscriptionId=8252</a> > in the United

States and Privacy International < <a href="https://www.privacyinternational.org/article/about-donating-pi">https://www.privacyinternational.org/article/about-donating-pi</a> > in Britain and Europe can help maintain a culture of strong privacy.

#### References

- [1] Jones and Soltren 2005
- [2] Valkenburg, Peter and Schouten 2006
- [3] Roeder 2011
- [4] Who's Watching? 2011
- [5] Rotenberg, et al. 2009
- [6] Leibowitz, et al. 2011, p 6
- [7] Beringer, et al. 2011
- [8] EPIC 2011

#### **Works Cited**

- Beringer, S. Ashlie, M. Sean Royall, Theodore W. Ullyot, Laura D. Berger, Cora Tung Han, and Manas Mohapatra. "In the Matter of Facebook, Inc.: Agreement Containing Consent Order." Federal Trade Commission. 29 11 2011. <a href="http://ftc.gov/os/caselist/0923184/111129facebookagree.pdf">http://ftc.gov/os/caselist/0923184/111129facebookagree.pdf</a> (accessed 12 23, 2011).
- EPIC. "Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises." Electronic Privacy Information Center. 29 11 2011. <a href="http://ftc.gov/opa/2011/11/privacysettlement.shtm">http://ftc.gov/opa/2011/11/privacysettlement.shtm</a> (accessed 12 23, 2011).
- Jones, Harvey, and Jose Hiram Soltren. Facebook: Threats to Privacy. 14 December 2005.

  <a href="http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf">http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf</a> (accessed November 30 2011).
- Leibowitz, Jon, J. Thomas Rosch, Edith Ramirez, and Julie Brill. "In the Matter of FACEBOOK, Inc.: FTC Ruling." Federal Trade Commission. 29 11 2011. <a href="http://ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf">http://ftc.gov/os/caselist/0923184/111129facebookcmpt.pdf</a> (accessed 12 23, 2011).
- Roeder, Linda. "How Much Information Is Too Much? Be Safe Online." about.com Social Media. 2011. <a href="http://personalweb.about.com/cs/securityprivacy/a/311toomuchinfo.htm">http://personalweb.about.com/cs/securityprivacy/a/311toomuchinfo.htm</a> (accessed 12 31, 2011).
- Rotenberg, Marc, John Verdi, Kimberly Nguyen, Jared Kaprove, Matthew Phillips, and Ginger McCall. "In the Matter of Facebook, Inc.: Complaint, Request for Investigation, Injunction, and Other Relief." Electronic Privacy Information Center. 17 12 2009. <a href="http://epic.org/privacy/inrefacebook/EPIC-Facebook/Complaint.pdf">http://epic.org/privacy/inrefacebook/EPIC-Facebook/Complaint.pdf</a> (accessed 12 23, 2011).
- Valkenburg, Patti M., Jochen Peter, and Alexander P. Schouten. "Friend Networking Sites and Their Relationship to Adolescents' Well-Being and Social Self-Esteem." *CyberPsychology & Behavior* 9, no. 5 (10 2006): 584-590. (Accessed 12 31 2011 through Norwich University Kreitzberg Library online databases.)
- Who's Watching? "Too Much Information: On social networking sites, you may be giving away more than you think." Who's Watching. 2011. <a href="http://whoswatchingcharlottesville.org/social.html">http://whoswatchingcharlottesville.org/social.html</a> (accessed 12 24, 2011).

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

\* \* \*

Copyright © 2012 Maria Dailey & M. E. Kabay. All rights reserved.

# **Future Privacy**

by Maria Dailey & M. E. Kabay, PhD, CISSP-ISSMP School of Business & Management Norwich University, Northfield VT

Maria Dailey is a senior in the Bachelor of Science in Computer Security and Information Assurance (BSCSIA) in the School of Business at Norwich University. She recently submitted an interesting essay in the IS455 Strategic Applications of Information Technology course, and I suggested to her that we work together to edit and expand it for publication. The following is the result of a close collaboration between us.

\* \* \*

How would you feel about having a computer insider your body – other than your own brain?

A nanocomputer is one which is invisible to the human eye, but operates like current computers.

"You might stop to consider what the world might be like, if computers the size of molecules become a reality. These are the types of computers that could be everywhere, but never seen. Nano sized bio-computers that could target specific areas inside your body. Giant networks of computers, in your clothing, your house, your car. Entrenched in almost every aspect of our lives and yet you may never give them a single thought."[1]

Nanotechnology research is proceeding vigorously:

- In 2001, Wired reporter Geoff Brumfiel wrote that researchers at Bell Labs reported that they had "built a Field-Effect Transistor (FET) from a single molecule." One of the researchers "said this special ability might allow computer circuits to become integrated into credit cards and clothing. The fact that the molecule can be stored easily in a liquid solution also opens up the possibility of using ink-jet type technology to 'print' processors on sheets of plastic."[2]
- Brumfiel also pointed to the startling achievement of researchers at Harvard University who "made semiconducting nanowires that assembled themselves into simple circuits." Luminary scientist Ralph Merkle,[3] one of the founders of modern cryptography, and currently a researcher in nanotechnology, commented explained to Brumfiel that "Molecular processors... could allow computers to see, hear and interact with humans much more directly."[2]
- In mid-2011, "A group of Turkish researchers at an Ankara university have manufactured the longest and thinnest nanowires ever produced, by employing a novel method to shrink matter 10-million fold." [4] Such nanowires could play a valuable role in nanoscale computing.
- A Website devoted to monitoring developments in nanoscale computing has the motto, "Small is beautiful; very small is very beautiful."[5] The current page alone has 30

entries on a multitude of nanotechnology topics, with more than a thousand more archived. Examples include

- o DNA Nanotechnology a basis for biologically-based nanocomputers;[6]
- Augmented Reality Microsoft and University of Washington scientists are working on contact lenses with digital displays providing additional information on demand;[7]
- O Building an Artificial Brain University of Southern California researchers "have made a significant breakthrough in the use of nanotechnologies for the construction of a synthetic brain. They have built a carbon nanotube synapse circuit whose behavior in tests reproduces the function of a neuron, the building block of the brain."[8]

The intimate integration of computing technology potentially goes far beyond anything citizens today would be comfortable accepting, if current concerns over data profiling are a basis for prediction.[9] Consumers already shift uncomfortably in their seats when highly personalized e-advertisements update each time they leave a Website.[10] How will they feel about computers that transmit even more intimate details of their lives?

Nanocomputers may challenge current conceptions of privacy, trust, and criminal boundaries. An embedded microscopic computer recording and transmitting details of its host's location, ambient sound, and perhaps even physiological markers would be a tool of great value for medicine, the criminal justice system, and marketing – and also for a police state's apparatus of surveillance and control. Imagine what organized crime or individual criminals could do with surreptitiously implanted nanocomputers! That accidental bump in the street could be an undetectable insertion of a tracking or monitoring nanodevice instead of the occasion for mere physical pickpocketing.[11]

Privacy would have to extend to envelop computerization of the human body. Nanocomputers hold the potential to alter cells and target certain diseases and illnesses[12] – but what if they were susceptible to unauthorized dumps of information about the carrier's state of health? For example, nanocomputers may someday be programmed to monitor, follow, and record individuals and groups for medical treatment or in research studies. The reports could be submitted to authorised health care workers and scientists – or they might be deliberately or covertly directed to marketers with or perhaps without the victim's awareness of the situation, much as marketers today monitor consumer online activity in social networking sites.[13] Maintaining privacy would require that trusted nanocomputers be programmed to act as firewalls against unauthorized activity, so that unsolicited monitoring and advertising could not take place.

What if criminal hackers attacked embedded nanocomputers in human beings? If a medical nanocomputer were not only recording medical data but, like today's cardiac pacemakers, providing useful or essential medical services (e.g., controlling heart rate, modifying endocrine functions, affecting brain functions), could unauthorized modification lead to harm? In 2008, there were reports that WiFi signals could interfere with – or be used to interfere with – cardiac pacemakers.[14] Recent reports discuss defensive methods for preventing such problems or attacks.[15]

If such systems were to be used to affect behaviour (think "A Clockwork Orange"[16]), how would one distinguish natural human behaviour and nanomanipulated actions? How would the system of justice cope with a "nanocomputer-made-me-do-it" defence argument?

Integrating security and social implications for privacy and autonomy into the design and applications of embedded nanocomputers must be a priority for all developers and users of this new technology.

These issue give a whole new meaning to the concept of a *small mistake*.

#### References

- [1] Future For All 2011
- [2] Brumfiel 2001
- [3] Computer History Museum 2011
- [4] TURKEY Tr-national 2011
- [5] NanoComputer 2012
- [6] Admin, DNA Nanotechnology 2012
- [7] Admin, Augmented Reality 2012
- [8] Admin, Building an Artificial Brain 2011
- [9] Privacy Rights Clearinghouse 2011
- [10] Folino 2009
- [11] Anonymous 2011
- [12] Dillow 2011
- [13] Jones and Soltren 2005
- [14] Claburn 2008
- [15] Storm 2011
- [16] IMDB 2012

#### **Works Cited**

- Admin. "Augmented Reality." NanoComputer: very small is very beautiful. 10 01 2012. http://www.nanocomputer.com/?p=1512 (accessed 01 15, 2012).
- —. "Building an Artificial Brain." NanoComputer: very small is very beautiful. 24 12 2011. http://www.nanocomputer.com/?p=94 (accessed 01 15, 2012).
- —. "DNA Nanotechnology." NanoComputer: very small is very beautiful. 13 01 2012. <a href="http://www.nanocomputer.com/?p=1540">http://www.nanocomputer.com/?p=1540</a> (accessed 01 15, 2012).
- Anonymous. "Pickpocket Pointers: 12 Methods to Do the Dip." Vice Beta. 2011. <a href="http://www.vice.com/read/pickpocket-v13n6">http://www.vice.com/read/pickpocket-v13n6</a> (accessed 01 15, 2012).
- Brumfiel, Geoff. "Nanocomputers Get Real." *Wired* | Science | Discoveries. 09 11 2001. http://www.wired.com/science/discoveries/news/2001/11/48278 (accessed 01 15, 2012).
- Claburn, Thomas. "Pacemakers Vulnerable To Hacking: Three medical schools demonstrate the wireless dangers that can disturb an implantable cardioverter defibrillator like the Medtronic Maximo DR." *InformationWeek*. 12 03 2008. http://www.informationweek.com/news/206903321 (accessed 01 15, 2012).
- Computer History Museum. "Ralph Merkle: 2011 Fellow Award Recipient." CHM Fellow Awards. 2011. <a href="http://www.computerhistory.org/fellowawards/hall/bios/Ralph,Merkle/">http://www.computerhistory.org/fellowawards/hall/bios/Ralph,Merkle/</a> (accessed 01 15, 2012).
- Dillow, Clay. "An Israeli Biocomputer Can Now Detect Multiple Signs of Disease from Inside the Body." POPSCI: The Future Now. 06 07 2011.

  <a href="http://www.popsci.com/science/article/2011-07/israeli-biocomputer-can-now-detect-multiple-signs-disease-inside-body">http://www.popsci.com/science/article/2011-07/israeli-biocomputer-can-now-detect-multiple-signs-disease-inside-body</a> (accessed 01 15, 2012).

- Folino, Lauren. "Internet Users Object to Tailored Ads: Study reveals bad news for companies that track online users in order to tailor advertising." Inc. | Topics | Technology Transfer. 08 10 2009. <a href="http://www.inc.com/news/articles/2009/10/tailored-ads.html">http://www.inc.com/news/articles/2009/10/tailored-ads.html</a> (accessed 01 15, 2012).
- Future For All. "Computers of Tomorrow." Future For All. 2011. http://www.futureforall.org/computers/computers.htm (accessed 01 15, 2012).
- IMDB. "A Clockwork Orange." Internet Movie Database. 2012. http://www.imdb.com/title/tt0066921/ (accessed 01 15, 2012).
- Jones, Harvey, and Jose Hiram Soltren. Facebook: Threats to Privacy. 14 December 2005. <a href="http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf">http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf</a> (accessed November 30 2011).
- NanoComputer. NanoComputer: very small is very beautiful. 13 01 2012. http://www.nanocomputer.com/ (accessed 01 15, 2012).
- Privacy Rights Clearinghouse. Privacy Today: A Review of Current Issues. 08 2011. <a href="https://www.privacyrights.org/ar/Privacy-IssuesList.htm#dataprofiling">https://www.privacyrights.org/ar/Privacy-IssuesList.htm#dataprofiling</a> (accessed 01 15, 2012).
- Storm, Darlene. "Jamming signals to stop hackers from lethal pacemaker attacks." 

  \*\*Computerworld\* | Security is Sexy. 23 08 2011.

  http://blogs.computerworld.com/18842/jamming\_signals\_to\_stop\_hackers\_from\_lethal\_p
  acemaker\_attacks (accessed 01 15, 2012).
- TURKEY Tr-national. "Turkish researchers make nanotechnology breakthrough." *Hurriyet Daily News.* 17 06 2011.

  <a href="http://www.hurriyetdailynews.com/default.aspx?pageid=438&n=turkish-researchers-make-nanotechnology-breakthrough-2011-06-17">http://www.hurriyetdailynews.com/default.aspx?pageid=438&n=turkish-researchers-make-nanotechnology-breakthrough-2011-06-17</a> (accessed 01 17, 2012).

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.



## Oil Industry Open to Cyberattacks

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

A colleague recently asked me how vulnerable oil-industry installations are to cyberattack; unfortunately, the consensus seems to be "Very."

In February 2011, a report surfaced that "Computer hackers working through Internet servers in China broke into and stole proprietary information from the networks of six U.S. and European energy companies, including Exxon Mobil Corp., Royal Dutch Shell Plc and BP Plc...." Other targets included "Marathon Oil Corp., ConocoPhillips and Baker Hughes Inc., .... [a] Houston-based provider of advanced drilling technology." Publicly traded oil-industry companies hacked by industrial spies or saboteurs might be sued by shareholders if they fail to disclose such attacks: "Investors might also argue they had a right under U.S. securities laws to be informed of the thefts, which a judge might construe as a 'material' fact that should have been disclosed...."

In an August 2011 report, Matt Liebowitz of the *SecurityNewsDaily* reported on a Black Hat Security Conference demonstration of hacking the programmable logic controllers (PLCs) used in many industrial systems including power plants and oil refineries.<sup>2</sup> Dillon Beresford, an expert penetration tester, found canonical (standard) passwords on a Siemens Simatic S7 PLC. He was able to shut down the controllers and also to "report false data to make the operator 'think that everything's functioning normal, when in fact it's not.""

The Duqu Trojan software detected in October 2011 by the anti-malware firm Symantec is "scarily similar to the infamous Stuxnet worm, which could disrupt computers controlling power plants, oil refineries and other critical infrastructure networks." Stuxnet is the worm that disabled the supervisory control and data acquisition (SCADA) systems in Iran's nuclear-fuel processing facility. "Symantec said whoever is behind Duqu rigged the Trojan to install another information-stealing program on targeted computers that could record users' keystrokes and system information and transmit them, and other harvested data, to a command-and-control (C&C) server."

In December 2011, a speaker from Shell Oil at "the World Petroleum Conference in Doha ... [said] ... that the company had suffered an increased number of attacks .... motivated by both commercial and criminal intent." The manager warned, ""If anybody gets into the area where you can control opening and closing of valves, or release valves, you can imagine what happens. It will cost lives and it will cost production, it will cost money, cause fires and cause loss of containment, environmental damage – huge, huge damage." The *FinancialMirror*, reporting on the same presentation, wrote that "Hackers are bombarding the world's computer controlled energy sector, conducting industrial espionage and threatening potential global havoc through oil

<sup>&</sup>lt;sup>1</sup> (Riley 2011)

<sup>&</sup>lt;sup>2</sup> (Liebowitz, How Easily Can a Power Plant Be Hacked? Very. 2011)

<sup>&</sup>lt;sup>3</sup> (Liebowitz, Stuxnet Clone Found Possibly Preparing Power Plant Attacks 2011)

<sup>&</sup>lt;sup>4</sup> (Zetter 2011)

<sup>&</sup>lt;sup>5</sup> (BBC 2011)

supply disruption. Oil company executives warned that attacks were becoming more frequent and more carefully planned." They added (quoting an interview):

"Cyber crime is a huge issue. It's not restricted to one company or another it's really broad and it is ongoing," said Dennis Painchaud, director of International Government Relations at Canada's Nexen Inc. "It is a very significant risk to our business. It's something that we have to stay on top of every day. It is a risk that is only going to grow and is probably one of the preeminent risks that we face today and will continue to face for some time."

Other speakers interviewed in the *FinancialMirror* story explained that cyberattacks could be used for financial gain: reducing the flow of oil could raise prices – and threats and incidents involving oil-industry installations could allow criminals and state-sponsored cyberattackers to profit using the futures market.

Readers interested in learning more about SCADA vulnerability testing will find a valuable resource by Joel Langill online at SCADAhacker.com, which includes dozens of professional papers by the penetration expert.<sup>7</sup>

#### **Works Cited**

- BBC. "Oil cyber-attacks could cost lives, Shell warns." *BBC News Technology*. 12 12, 2011. http://www.bbc.co.uk/news/technology-16137573 (accessed 01 15, 2012).
- FinancialMirror. "Cyber attacks could wreck world oil supply." *FinancialMirror | News | Business & Economy.* 12 11, 2011. http://www.financialmirror.com/news-details.php?nid=25208# (accessed 01 15, 2012).
- Langill, Joel. "About SCADAhacker." *SCADAhacker*. 01 13, 2012. http://scadahacker.com/about.html (accessed 01 15, 2012).
- Liebowitz, Matt. "How Easily Can a Power Plant Be Hacked? Very." *securitynewsdaily*. 08 03, 2011. http://www.securitynewsdaily.com/how-easily-can-a-power-plant-be-hacked-very-1023/ (accessed 01 15, 2012).
- —. "Stuxnet Clone Found Possibly Preparing Power Plant Attacks." *securitynewsdaily*. 10 18, 2011. http://www.securitynewsdaily.com/stuxnet-clone-found-preparing-power-plant-attacks-1250/ (accessed 01 15, 2012).
- Riley, Michael. "Exxon, Shell, BP Said to Have Been Hacked Through Chinese Internet Servers." *Bloomberg.* 02 24, 2011. http://www.bloomberg.com/news/2011-02-24/exxon-shell-bp-said-to-have-been-hacked-through-chinese-internet-servers.html (accessed 01 15, 2012).
- Zetter, Kim. "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History." *Wired.* 07 11, 2011. http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1 (accessed 01 15, 2012).

\* \* \*

<sup>&</sup>lt;sup>6</sup> (FinancialMirror 2011)

<sup>&</sup>lt;sup>7</sup> (Langill 2012)

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

Copyright © 2011 M. E. Kabay. All rights reserved.

Permission is hereby granted to *InfoSec Reviews* to post this article on the *InfoSec Perception* Web site in accordance with the terms of the Agreement in force between *InfoSec Reviews* and M. E. Kabay.

## **IA Includes Software Development**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Sometimes we lose sight of the wide reach of information assurance (IA). In class discussions in the Management of IA course< <a href="http://www.mekabay.com/courses/academic/norwich/is342/index.htm">http://www.mekabay.com/courses/academic/norwich/is342/index.htm</a> at Norwich University< <a href="http://www.norwich.edu">http://www.norwich.edu</a> >, students recently discussed how software development and quality assurance play a role in IA.

One of the areas that our students study in their software engineering courses <a href="http://www.mekabay.com/courses/academic/norwich/is301/">http://www.mekabay.com/courses/academic/norwich/is301/</a> > is development strategies <a href="http://www.mekabay.com/courses/academic/norwich/is301/04">http://www.mekabay.com/courses/academic/norwich/is301/04</a> ch4.ppt >. The traditional system development life cycle (SDLC) puts a great deal of time and effort into the project definition phases; systems analysts must interact with users, encourage them to define their needs, define functional requirements (these two phases can be called the requirements elicitation), get the functional specifications approved by the users, and then design and build the systems to meet those requirements. The SDLC includes system testing and system documentation.

An alternative is agile development < http://www.allaboutagile.com/10-key-principles-of-agile-softwaredevelopment/>, which can include rapid application development (RAD< http://www.cs.bgsu.edu/maner/domains/RAD.htm >) and joint application development (JAD< http://www.umsl.edu/~sauterv/analysis/JAD.html >). In these methods< http://www.mekabay.com/courses/academic/norwich/is301/23\_ch17.ppt >, analysts follow the requirements elicitation phase by model-building (prototypes). Prototypes< http://csweb.cs.bgsu.edu/maner/domains/Proto.htm > can be created with simple development tools that allow users to see partial or even simulated user interfaces with some of their required functions enabled by fourth-generation languages (4GLs) or application generators. Faced with a model or simulation of functions that can meet their needs - at least, in part - users often respond with corrections and clarifications, thus helping analysts understand and document user needs more thoroughly. Analysts can thus generate improved definitions of the functional requirements and support designers and programmers in building systems that better meet the organization's needs. In addition, agile development methodologies can provide a significant degree of preliminary functionality early in the development cycle, immediately meeting some of the most common needs within weeks or months instead of forcing everyone to wait for all the functionality to be released in the months or even years typically forced by the traditional SDLC.

Decades ago, I defined a rule to describe the effect on users of seeing a model that simulates part of a new system: the availability of a tool changes the perception of the possible. I defined that principle partly because of an incident that occurred in 1986, when I was hired to help reorganize the information technology operations of a clothing factory, with special attention on performance and technical support. As I was walking through the office with the vice-president (VP) of information technology (IT), I noticed something unusual off to one side of the office: there was an employee with a thick stack of 132-character by 88-line computer printouts working with a hand calculator. I asked the VP if we could go talk to him and then asked him politely what he was doing. He said he was calculating subtotals based on the printouts. "Ah," I said, "and how often do you do that?" He said he did it every month. "How long does it take you?" A few hours. "And how long have you been doing that?" About three years. Finally, I asked, "Have you ever asked your IT department to include the subtotals in your report?"

The employee looked at me in blank astonishment.

#### "They can DO that?!?"

One point of the story is that everyone in IT has to focus on user needs and actively interact with users not only to ask them about their perceived needs but also to stimulate cooperation in thinking clearly about all the functional requirements of IT systems, whether they are currently recognized or not. IT staff are supposed to be the experts who are aware of requirements that the users may never have thought about; one of the key areas where users who are focused on their own work either forget to define requirements or are completely unaware of them is security.

Security requirements – protection of confidentiality, control, integrity, authenticity, availability and utility of information – *must* be included in the functional specifications of *every* IT system. Ignoring security considerations for software is like ignoring safety considerations in automobiles: it's unprofessional and potentially dangerous. The Risks Forum Digest has documented thousands of systems over more than two decades in which security considerations were either ignored, poorly defined, or poorly implemented. The year 2000 (Y2K) problem illustrated far-reaching consequences of failure to plan for continued utility and integrity in computer software – thousands of programs all over the world were at risk of failing because they used two-digit date fields that assumed that all dates would be in the 20th century only.

By now, most readers are surely aware that security must be built into systems from the very first, not simply added in as afterthoughts.

As programmers build the systems that meet user requirements, they must apply thorough software quality assurance (SQA) techniques. Many of the problems that SQA tries to find include errors that can profoundly affect security. A brief list includes

- Initialization Errors
- Logic Flow Errors
- Calculation Errors
- Boundary Condition Violations
- Parameter Passing Errors
- Race Conditions
- Load Conditions
- Resource Exhaustion
- Interapplication Conflicts
- Other Technical Errors
- Regulatory Compliance Considerations

For details of these issues, readers are invited to download the PDF or PPTX versions of our class notes, which are based on Chapter 39 of the *Computer Security Handbook*, 5th Edition < <a href="http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529">http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529</a> >, "Software Development and Quality Assurance," by John Mason, Jennifer Hadley, and Diane E. Levine.

In the next column, I'll review how patch management plays a critical role in information assurance.

\* \* \*

M. E. Kabay, < <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials. <a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

Copyright © 2011 M. E. Kabay. All rights reserved. Permission is hereby granted to *InfoSec Reviews* to post this article on the *InfoSec Perception* Web site in accordance with the terms of the Agreement in force between *InfoSec Reviews* and M. E. Kabay.

# Patch Management a Constant Requirement for IA

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

As operations staff run computer systems for mission-critical functions, they must constantly adapt to changing threats and newly discovered vulnerabilities – including vulnerabilities rooted in program design or implementation. In a recent session of the Management of Information Assurance (IA) course< <a href="http://www.mekabay.com/courses/academic/norwich/is342/index.htm">http://www.mekabay.com/courses/academic/norwich/is342/index.htm</a> at Norwich University< <a href="http://www.norwich.edu">http://www.norwich.edu</a>>, we spent an hour discussing how patch management supports IA.

Programs affect all six fundamental elements of IA – protection of confidentiality, control, integrity, authenticity, availability and utility of information < <a href="http://www.mekabay.com/overviews/hexad\_ppsx.zip">http://www.mekabay.com/overviews/hexad\_ppsx.zip</a> >. Manufacturers and volunteer programmers in the open-source < <a href="http://www.opensource.org/">http://www.opensource.org/</a> > movement issue tools for fixing problems in their code. These *patches* can include executable code to alter the machine-code of executable files, code to replace parts of existing code, or code to replace entire units of programs (e.g., dynamic link libraries <a href="http://msdn.microsoft.com/en-us/library/windows/desktop/ms682589(v=vs.85).aspx">http://msdn.microsoft.com/en-us/library/windows/desktop/ms682589(v=vs.85).aspx</a> > or DLLs). Microsoft issues patches for Windows on the second and fourth Tuesdays of each month. <a href="http://support.microsoft.com/kb/894199">http://support.microsoft.com/kb/894199</a> >

Some programs or utilities can automatically update target programs. For example, the Windows Update < <a href="http://windows.microsoft.com/en-US/windows/help/windows-update">http://windows.microsoft.com/en-US/windows/help/windows-update</a> > function allows beginners or amateurs to let the manufacturer of their operating system and other products receive and even install updates without manual intervention if they so choose. Since many millions of users lack the technical knowledge and awareness of possible problems that might influence them to delay installation of updates, this solution is a reasonable response to the constantly evolving threats and vulnerabilities of their systems.

Although individual users may choose to allow their products to auto-update, more experienced users and professionals managing mission-critical computers may choose to delay installation of patches as a function of their perceived urgency for those systems. Installing patches immediately may lead users into trouble as errors in the patches. For example, *Computerworld* blogger Michael Horowitz pointed out in February 2010<
<a href="http://blogs.computerworld.com/15581/microsoft fails its customers after a bad\_patch">http://blogs.computerworld.com/15581/microsoft fails its customers after a bad\_patch</a> that a Windows XP patch prevented some systems from rebooting.<
<a href="http://answers.microsoft.com/en-us/windows/forum/windows\_xp-windows\_update/blue-screen-error-0x0000007b-in-windows-xp-after/73cea559-ebbd-4274-96bc-e292b69f2fd1">http://answers.microsoft.com/en-us/windows/forum/windows\_xp-windows\_update/blue-screen-error-0x0000007b-in-windows-xp-after/73cea559-ebbd-4274-96bc-e292b69f2fd1</a> Horowitz wrote, "As you might expect of Defensive Computing oriented techie, I make a full image backup before running Windows/Microsoft update. I also wait a couple days before installing newly released patches...."

When I ran operations in a service bureau in the mid-1980s, the more critical the system, the longer we waited before installing patches and software revisions; the more critical the problem solved by such changes, the sooner we installed them. We used discussion groups and vendor notices to evaluate the reliability of patches and versions; unless we needed the changes (for example, to install new hardware not supported by the older software), we usually waited *six months* to see how our fellow system users world-wide coped with the changes. Like Horowitz, we took our time in testing the new software; we'd switch disk packs in our old 404MB washing-machine-sized disk drives and test the new programs on copies of our production data, not on the real data, for several days. Then if I decided to go ahead with the updates, we'd take double full backups and then install the new programs on a Friday night. Tests involving two or three customer employees from the 28 companies using our systems would run all of Saturday and Sunday, with a go/no-go decision by Sunday afternoon. If we continued with the new software, we'd have the entire technical support team on high alert and monitor operations throughout the client base for several days after the installation.

The systems we were using in the mid-1980s at my employer's company were multi-million-dollar minicomputers – huge by today's standards in terms of physical size (refrigerator- and compact-car-sized) and puny in terms of memory (megabytes, not gigabytes) and disk storage (our biggest drive – the size of a washing machine – held 404 megabytes in 1986). We had four minicomputers, three of which were identical. Managing patches was a manual task for one operator. However, in today's environments, there may be so much variety in installed software on servers and workstations that manually keeping track of all the required updates and patches can be impossible. Automated patching solutions< <a href="http://www.networkcomputing.com/servers-storage/229605578">http://www.networkcomputing.com/servers-storage/229605578</a> > allow system managers to track all the software on every system, including precise information about versions; using such information, a Patch and Vulnerability Group (PVG) can accomplish the following tasks without conflicts and confusion:

- Creating a system inventory
- Monitoring for vulnerabilities, remediations & threats
- Prioritizing vulnerability remediation
- Creating organization-specific remediation db
- Testing remediations
- Deploying vulnerability remediations
- Distributing vulnerability & remediation info to administrators
- Verifying remediation
- Vulnerability remediation training for new staff.

For additional details of patch and vulnerability management, see Chapter 40, "Managing Patches & Vulnerabilities" by Peter Mell and Karen Kent Scarfone in the *Computer Security Handbook*, 5th Edition< <a href="http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529">http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529</a> >. Class notes summarizing key points of the chapter are freely available online as PPTX<

http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch40\_patches.p ptx > and PDF<

 $\underline{http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch40\_patches.p} \\ \underline{df} > files.$ 

\* \* \*

M. E. Kabay, < <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials. <a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2011 M. E. Kabay. All rights reserved. Permission is hereby granted to *InfoSec Reviews* to post this article on the *InfoSec Perception* Web site in accordance with the terms of the Agreement in force between *InfoSec Reviews* and M. E. Kabay.

## **Resources for Creating Effective Security Policies**

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

Managing information assurance (IA) effectively and efficiently depends on defining our goals clearly, laying out how we will achieve our goals, and defining metrics by which we can tell if we are succeeding.

In a recent session of the Management of Information Assurance (IA) course<
<a href="http://www.mekabay.com/courses/academic/norwich/is342/index.htm">http://www.mekabay.com/courses/academic/norwich/is342/index.htm</a> at Norwich University<
<a href="http://www.norwich.edu">http://www.norwich.edu</a> , students and I spent an hour discussing how to define and apply fundamental concepts of security policy.

Four terms recur in discussions of all forms of IA management: the word *policy* itself, *controls*, *standards*, and *procedures*.

- *Policy* defines how what we intend to accomplish to protect information;
- Controls define the general approaches for implementing the desired protection;
- *Standards* stipulate specific and widely accepted measures for how well we implement controls consistent with policy; and
- *Procedures* define the specific operations we must carry out to meet standards in achieving the controls that reflect policy.

Typically, we segregate these four elements of IA management: policy is defined as a high-level definition that evolves relatively slowly – perhaps with quarterly or annual reviews by upper management. Controls and standards should be adjustable by line management (e.g., an information security officer) without having to bother upper managers (e.g., the chief information security officer or chief information officer) but subject to periodic review. Procedures ought to be adjustable by staff to meet conditions that can change from day to day as new threats and vulnerabilities are discovered; no one wants to have to ask an upper manager whether it's acceptable to warn users about a new phishing trick that appeared this morning.

Defining security policy benefits from careful attention to industry best practices as defined in a variety of standards documents; however, it's impossible to use standards rigidly, like a child following a recipe for cookies. The resources are tools for intelligent analysis and judgement; rather than trying to apply any one set of standards rigidly, it's to the policy-makers' benefit to consider alternatives and choose thoughtfully.

One of the families of standards that has become widely accepted in recent decades started with British Standard (BS) 7799 in 1995, which led to BS 7799v2 in 1999 and then the International Organization for Standards (ISO) 17799 of 1999 and later the ISO 17799:2005. By 2009, the ISO and the International Electrochemical Commission (IEC) had defined a family of information security standards called the ISO/IEC 27000. Some ISO standards are freely available for download < <a href="http://standards.iso.org/ittf/PubliclyAvailableStandards/">http://standards.iso.org/ittf/PubliclyAvailableStandards/</a> > but most cost about 100 Swiss Francs (CHF) or roughly 83 Euros or about U\$109 each. All of these documents can be purchased as PDF files (or as paper documents, although I have no idea why

anyone would want to buy a paper copy when one can simply print from the PDF) by using the IEC Webstore< <a href="http://webstore.iec.ch/">http://webstore.iec.ch/</a> and entering the standard number (e.g., 27000) into the Search field on the upper right of the page. In addition, there's a 50% educational discount available<

http://webstore.iec.ch/Webstore/webstore.nsf/0/C6B6F00BE9D89ED5C125761F0055DD41?OpenDocument > for orders submitted on academic institutional letterhead. For networked access by different numbers of users in one organization, special discounts< http://webstore.iec.ch/Webstore/webstore.nsf/0/F435E5A7A69B11E9C1257556005A62F1?OpenDocument > apply; for example, 20 users can access a document bought at only four times the individual-copy rate.

The overview of ISO/IEC 27000:2009 is available free in English from < <a href="http://standards.iso.org/ittf/PubliclyAvailableStandards/c041933\_ISO\_IEC\_27000\_2009.zip">http://standards.iso.org/ittf/PubliclyAvailableStandards/c041933\_ISO\_IEC\_27000\_2009.zip</a> > which contains a 26 page summary of most of the 27000 series of standards (those that existed as of 2009).

Page 12 of that document shows a map of the entire series in 20909, which included the following elements. Key components of the 27000 series include the following:

- ISO/IEC 27000 Overview and Vocabulary
- ISO/IEC 27001 Requirements
- ISO/IEC 27002 Code of Practice
- ISO/IEC 27003 Implementation Guidance
- ISO/IEC 27004 Measurement
- ISO/IEC 27005 Risk Management
- ISO/IEC 27006 Certification Body Requirements
- ISO/IEC 27007 Audit Guidelines
- ISO/IEC 27011 Telecommunications Organizations
- ISO 27799 Health Organizations

Additional standards in the series include

- ISO/IEC 27031 Business Continuity
- ISO/IEC 27033-1 Network Security
- ISO/IEC 27035 Security Incident Management

Another important resource for policy writers is CobiT: the Control Objectives for Information and Related Technologies< <a href="http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx">http://www.isaca.org/Knowledge-Center/cobit/Pages/Overview.aspx</a> > managed by ISACA< <a href="https://www.isaca.org/">https://www.isaca.org/</a> > (formerly the Information Systems Audit and Control Association). The group describes the standard as follows:

COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations. COBIT emphasizes regulatory compliance, helps organizations to increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework.

COBIT 5 is the forthcoming new version:

Schedule to release in 2012, COBIT 5 will consolidate and integrate the COBIT 4.1, Val IT 2.0 and Risk IT frameworks and also draw significantly from the Business Model for Information Security (BMIS) and ITAF.

Another valuable source of guidance in framing policies is the extensive set of documents from the Computer Emergency Response Team Coordination Center (CERT-CC< <a href="http://www.cert.org">http://www.cert.org</a> >) at the Software Engineering Institute of Carnegie Mellon University. The site has extensive documents and podcasts to help policy makers think about best practices and how to apply them to their specific organization's needs. Major sections worth exploring include Software Assurance, Security Systems, and Organizational Security.

A commercial tool for security-policy developers is Charles Cresson Wood's<
<a href="http://www.linkedin.com/pub/charles-cresson-wood/0/236/b99">http://www.linkedin.com/pub/charles-cresson-wood/0/236/b99</a> Information Security Policies
Made Easy (ISPME< <a href="http://www.informationshield.com/ispmemain.htm">http://www.informationshield.com/ispmemain.htm</a> ), which is in its 12<sup>th</sup> edition. I first used early editions of Wood's work in the 1980s for many policy-development contracts; some clients initially objected to the cost of a license (\$800) but I argued strongly that the book (and in later editions, CD-ROM) would save an immense amount of work and pay for itself within a few hours of work. One of the key features of the work is that Woods brilliantly provides alternatives – some of them outright contradictions of each other – for many policies and explains the reasons for choosing one or the other.

Tom Peltier's< <a href="http://www.linkedin.com/pub/thomas-peltier/1/536/ba5">http://www.linkedin.com/pub/thomas-peltier/1/536/ba5</a> > text, Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management < <a href="http://www.crcpress.com/product/isbn/9780849311376">http://www.crcpress.com/product/isbn/9780849311376</a> > is another useful resource for policy writers. This relatively short (312 pages) book is clearly organized and rooted in the author's experience in the field. Peltier's text was one of the reasons I hired him as one of the earliest instructors in the Master of Science in Information Assurance (MSIA<a href="http://infoassurance.norwich.edu/">http://infoassurance.norwich.edu/</a> >) program many years ago.

Class notes on Chapter 44, "Security Policy Guidelines," from the *Computer Security Handbook*, 5<sup>th</sup> edition< <a href="http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529/">http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529/</a>>, are freely available in PPTX<

 $\frac{http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch44\_security\_p}{olicy\_guidelines.pptx} > and PDF <$ 

http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch44\_security\_p\_olicy\_guidelines.pdf >.

*In the next article, I'll discuss some aspects of policy style.* 

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2011 M. E. Kabay. All rights reserved.

Permission is hereby granted to *InfoSec Reviews* to post this article on the *InfoSec Perception* 

Web site in accordance with the terms of the Agreement in force between <i>InfoSec Reviews</i> and M. E. Kabay.

# The Psychology of Decision-Making and Risk

by John Laskey & M. E. Kabay, PhD, CISSP-ISSMP

The following article is a contribution from John Laskey. Everything that follows is entirely John's work with minor edits from Mich.

Good risk management is fundamental to the security profession. When risks are overlooked or underplayed they can have a direct impact on a business and its reputation. When risks are overplayed, security becomes an inhibitor to productivity and challenges our credibility as professionals. And whenever security is seen as unnecessary, wasteful or uncompetitive then the stock of all security professionals goes down.

Sophisticated tools have been developed to assess security risks. The complexity and responsiveness of these tools require good levels of trust and understanding between security professionals – who understand the risk – and senior executives – who own the assets at risk. So if we wrap up the tools, the experts and the executives inside a good governance structure then we ought to get good security. But there's something missing.

A few years back I sat in a theatre of over 200 senior government security managers and professionals on a three day seminar. One session was different: it was about psychology. The speaker emphasised how the decisions we make about security were influenced by personal perception rather than real likelihood.

To illustrate this he gave the audience a hand-out describing a risk-related problem. Those on the right were given a version described in terms of the savings involved in the situation while those on the left were given the same information but described in terms of the losses involved. From a risk analysis standpoint both versions were identical, only the way the information was being presented was different. However, this seemingly trivial difference in wording radically changed risk attitudes. When asked to choose which of two actions to take those on the right (given the saving version) strongly preferred the safe option while those on the left (given the loss version) strongly preferred the risky option. It was a revelation. Unwittingly we experts had shown how our powers of decision-making and our attitudes to risk were influenced by how information is presented. The speaker showed how a range of other psychological factors can affect how we perceive and act in the face of risk.

The speaker was John Maule <a href="http://business.leeds.ac.uk/about-us/faculty-staff/member/profile/john-maule/">http://business.leeds.ac.uk/about-us/faculty-staff/member/profile/john-maule/</a>, who is Emeritus Professor of Human Decision-Making at Leeds University Business School, England. Maule has been active in heightening public awareness about the limitations to the intuitive judgement of risk. To this end he has submitted written evidence to a Select Committee of UK Lawmakers on Economic Affairs<
<a href="http://www.publications.parliament.uk/pa/ld200506/ldselect/ldeconaf/183/183we19.htm">http://www.publications.parliament.uk/pa/ld200506/ldselect/ldeconaf/183/183we19.htm</a>. He argued for greater awareness of the often personal, emotional responses that can shape and drive law-making. Maule has also highlighted the role of personal perception in response to fears of terrorism. In the aftermath of the 2005 Al-Qaida inspired bomb attacks on London's transportation system in which over 50 people were killed and over 700 injured, the BBC noted that many more London commuters were now choosing to walk or cycle. Maule argued that this was because such methods gave commuters the feeling of being more in control, not because it actually made them safer. For a generalised comparison, UK government figures for 2005 < UK

government figures for 2005 <

http://webarchive.nationalarchives.gov.uk/%2B/http%3A/www.dft.gov.uk/adobepdf/162469/221 412/221549/227755/roadcasualtiesgreatbritain2005a >show 372 pedal cyclists and 1224 pedestrians were killed or seriously injured in accidents in the greater London area (Table 46a, page 116 in text). No such figures were cited by Maule, but he held that graphic media coverage<a href="http://www.guardian.co.uk/flash/page/0%2C%2C1808096%2C00.html">http://www.guardian.co.uk/flash/page/0%2C%2C1808096%2C00.html</a> of the attacks had lodged in the minds of London commuters, making them feel that travelling on the subway was much riskier than it really was. This led them to take action that actually *increased* rather than decreased their exposure to risk.

Maule also holds an interesting view on group involvement in decision-making. In a published response < <a href="http://www.independent.co.uk/opinion/letters/letters-the-hs2-project-2053404.html">http://www.independent.co.uk/opinion/letters/letters-the-hs2-project-2053404.html</a> to a particular theory ("Nudge theory is only short term") he argued that "...when people are actively involved in making a decision they are more committed to it and will stick to it longer, even when the outcomes are not as good as expected." This observation should reassure those of us who worry whether senior executives have the time or inclination to grasp the more complex points of our art.

This analysis of human risk perception might paint a rather bleak picture. After all, we must use complex risk assessment tools that are the domain of experts. Then we have to put our conclusions into language that non-experts with high degrees of responsibility can grasp. And now Professor Maule tells us that we also need to think much more about the way we draw our conclusions on risks. Indeed, in a recent book (*Decision Behaviour, Analysis and Support*<
<a href="http://www.amazon.com/Decision-Behaviour-Analysis-Support-French/dp/0521709784/">http://www.amazon.com/Decision-Behaviour-Analysis-Support-French/dp/0521709784/</a>>)
Maule and his co-authors (Simon French and Nadia Papamichail) describe a range of techniques for improving thinking in risk situations. Though we know that security management can work and that our security experts do their jobs well and in the interests of the business, there are lessons for all of us in Maule's work.

I think we just need to take a little more time to ask ourselves whether we are worrying about the right things and reacting to them in a proportionate and timely way. In addition, we need to reflect more on how we are thinking and to develop our understanding beyond our first thoughts and impressions.

\* \* \*

John G Laskey< <a href="http://www.linkedin.com/pub/john-laskey/28/b28/b69">http://www.linkedin.com/pub/john-laskey/28/b28/b69</a> > is a British security consultant who has worked for the UK government in national security and emergency response since 1986. As IT Security Officer for the Home Office he was responsible for the security risk management of a number of high profile systems developed to increase government and public security. John is a founder of and assessor for the UK government Infosec Training Paths and Competencies (ITPC)<a href="https://www.instisp.org/SSLPage.aspx?pid=422">https://www.instisp.org/SSLPage.aspx?pid=422</a> > scheme from the Institute of Information Security Professionals</a> <a href="http://www.instisp.org">http://www.instisp.org</a> > that formally certifies those working in UK government information security projects. In addition to his experience in project security and security awareness, John has advised senior government managers on the health of major projects and programmes and he is a certified lead auditor for the ISO 27001 security standard. He is also a member of BCS, the Chartered Institute for IT<<a href="http://www.bcs.org/">http://www.bcs.org/</a> > and of the Security Institute<<a href="http://www.security-institute.org/">http://www.security-institute.org/</a>>.

\* \* \*

operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< <a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

Copyright © 2012 John Laskey & M. E. Kabay. All rights reserved.

# **Security-Policy Style**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

### Why Does Style Matter?

One of the major areas of my work and operations management has been the development and refinement of information-security policies. Over the years, I have seen cases in which well designed policies have been implemented in effectively in part because of style of presentation. Style is defined in the Encarta Dictionary as a "way of writing or performing: the way in which something is written or performed, as distinct from its content." Style includes the wording and tone, organization, presentation, and even maintenance of the policies. Style influences the reception and effectiveness of policies.

### **Writing the Policies**

Policies should include both prescriptive and proscriptive content; that is, the policy should describe both what people should do and what people should not do in clear, definite, and unambiguous style. Policy writers should aim for short, simple declarative sentences rather than long, complex, meandering sentences. Every policy should include a simple explanation of its purpose; additional explanations in more depth should be available as optional hyperlinks. Policy handbooks should include several ways of locating specific policies; e.g., detailed table of contents, multilevel headings throughout the text, and extensive indexes.

### **Organizing the Policies**

Policies should be made available in multiple formats. The topical organization presents policies in a sequence corresponding to an overall conception of security goals. For example, one can organize security policies starting at the external perimeter (physical security issues such as facilities protection, employee identification and authentication for physical access, and loss-prevention policies) and work inwards.

Special-purpose documents focusing on the security needs of particular groups are another view of the security policies. It is pointless to provide secretarial pool with policies defining internal firewall policies; it's a waste of time to inflict details of separation of duty in accounting functions on the helpdesk staff. Security policy documents should be useful and relevant to the groups for which they are compiled.

All the policies should be structured hierarchically; i.e., they should start with a general description and present increasing detail at lower levels of the policy document. For example, the security-policy section of Charles Cresson Wood's *Information Security Policies Made Easy* < <a href="http://www.informationshield.com/ispmemain.htm">http://www.informationshield.com/ispmemain.htm</a> > (Section 3 in the 10<sup>th</sup> Edition) starts with the following topics:

- 1.1 Information protection
- 1.2 Use of information
- 1.3 Information handling, access and usage
- 1.4 Data and program damage disclaimers
- 1.5 Legal conflicts
- 1.6 Exception to policies
- 1.7 Policy non-enforcement
- 1.8 Violation of law
- 1.9 Revocation of access privileges
- 1.10 Industry-specific information security standards
- 1.11 Policy-driven information system security architecture
- 2 Review and evaluation
  - 2.1 Security controls enforceability

### **Presenting the Policies**

Two decades ago, most of the organizations I worked with used paper documents for their policies. Typically, employees would receive huge loose-leaf binders for the policies; some organizations also used short paper documents for specific purposes and even reference cards, summary sheets, stickers and posters to communicate their policies. Updating this material was a nightmare: one would often see the security binder topped with stacks of unopened envelopes containing quarterly updates that employees were supposed to manually insert into their binders to replace outmoded policies and include new ones. There's nothing wrong with providing cute, clever reminder cards or attractive posters reminding people of security policies as part of a security awareness campaign; however, expecting employees to maintain paper versions of policies that most see as secondary to their work is unrealistic.

Electronic versions of policies are far more effective in my opinion than any paper compilation can be. In addition, electronic policies offer hypertext, whether in HTML or XML, RTF and word-processor files, or PDFs and HELP files. Links allow users to find material quickly, reducing irritation and frustration when looking for specific policies.

### **Maintaining the Policies**

I strongly recommend that every organization commit to continuous process improvement. For security policies, it should be easy for employees to suggest improvements in any aspect of policies. A committee that includes representatives from throughout the organization should meet periodically to consider those suggestions an update the policies as appropriate. The proposed changes should be circulated as draft for input; such exposure can contribute to a legitimate sense of policy ownership for employees. Major changes should be announced by upper management with an emphasis on explanations of those changes. If the policies are always available online rather than being printed, the changes will be instantly visible.

Class notes on Chapter 44, "Security Policy Guidelines," from the *Computer Security Handbook*, 5th edition< <a href="http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529/">http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529/</a>>, are freely available in PPTX<

http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch44\_security\_p\_olicy\_guidelines.pptx > and PDF<

http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch44\_security\_policy\_guidelines.pdf >.

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2012 M. E. Kabay. All rights reserved.

### **CobiT 5.0 Due for Release**

### by Pritam Bankar, CISA, CISM & M. E. Kabay, PhD, CISSP-ISSMP

Security professionals should constantly monitor developments in information technology (IT) governance for ideas that can support our work in developing, implementing, and monitoring information security. Today we have an overview of recent changes in the CobiT framework for IT governance from Pritam Bankar, CISA, CISM. What follows is entirely Mr Bankar's work with minor edits.

The Control Objectives for Information and Related Technology (CobiT) is a set of best practices (framework) for information technology (IT) Management & Governance. CobiT helps organizations meet today's business challenges in regulatory compliance, risk management and alignment of IT strategy with organizational goals. The first version was published by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute in 1996.

CobiT 4.1< <a href="http://www.isaca.org/Knowledge-Center/CobiT/Documents/CobiT4.pdf">http://www.isaca.org/Knowledge-Center/CobiT/Documents/CobiT4.pdf</a> was published in 2007 to provide IT practitioners and mangers with an IT governance model to deliver value from IT and to manage risks associated with IT. CobiT 4.1 is currently being updated to 5.0< <a href="http://www.isaca.org/Knowledge-">http://www.isaca.org/Knowledge-</a>

Center/Research/ResearchDeliverables/Pages/CobiT-5-Exposure-Draft.aspx > and will consolidate and integrate various frameworks like CobiT 4.1, Val IT 2.0 <a href="http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT1.aspx">http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT1.aspx</a>, RISK IT <a href="http://www.isaca.org/Knowledge-Center/Research/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx">http://www.isaca.org/Knowledge-Center/Research/Research/Research/Research/Research/Research/Research/Research/Research/Research/Pages/ITAF-A-Professional-Practices-Framework-for-IT-Assurance.aspx</a> > to create a detailed framework for effective governance and management of IT. CobiT 5.0 is scheduled to be released in 2012.

### **CHANGES FROM 4.1**

#### 1. Stakeholder Expectations and Value Driven

The main driver behind CobiT 5.0 is stakeholder expectations and values. These changes ensure that the needs of both internal and external customers are considered in addition to the enterprise strategy and goals which are currently emphasized 4.1for benefits realization, risk balancing and cost optimization.

### 2. Domain Areas

CobiT 5 has five domains under governance and management. The governance section provides guidance on evaluation, direction and monitoring of IT processes and is aligned with the ISO38500< <a href="http://www.38500.org/">http://www.38500.org/</a> > standard for "standard for corporate governance of information technology." The four domains in the management area are

- Align, Plan and Organize
- Build, Acquire and Implement
- Deliver, Service and Support
- Monitor, Evaluate and Assess

Even though the names have changed, the management domains are in line with the four equivalent domains of CobiT 4.1.

#### 3. Process Model and Areas

CobiT 5.0 has 36 processes (CobiT 4.1 has 34). A few processes from CobiT 4.1 are merged in 5.0 and some single processes from 4.1 are split to form separate processes in 5.0 to allow for more specific guidance. For example, ME4 – *Provide it Governance* from CobiT 4.1 is split into five separate processes (EDM1 to EDM5) under the new *Governance Domain*. Two new processes are introduced:

- AP01- Define Management Framework for IT
- BA18 Knowledge Management.

### 4. Integrated Framework

Different frameworks such as Val IT, Risk IT, BMIS, ITAF and relevant data points from various standards and best practices from organization such as ISO<
<a href="http://www.iso.org/iso/iso\_catalogue.htm">http://www.iso.org/iso/iso\_catalogue.htm</a> >, ITIL<<a href="http://www.itil-officialsite.com/">http://www.itil-officialsite.com/</a> >, PMBOK<<a href="http://www.opengroup.org/PMBOK-Guide-and-Standards.aspx">http://www.opengroup.org/PMBOK-Guide-and-Standards.aspx</a> >, TOGAF<<a href="http://www.opengroup.org/togaf/">http://www.opengroup.org/togaf/</a> > and CobiT 4.1 are consolidated into a single framework providing a single source of guidance. This integration will support a holistic view of management and governance in the enterprise.

### 5. Capability / Maturity Model

CobiT 4.1 has a process maturity model to assess the maturity of current state of enterprise and identify the steps to improve the process to achieve desired maturity level. This older maturity model is replaced by a process capability model based on ISO 15504<
<a href="http://www.iso.org/iso/iso\_catalogue/catalogue\_tc/catalogue\_detail.htm?csnumber=38932">http://www.iso.org/iso/iso\_catalogue/catalogue\_tc/catalogue\_detail.htm?csnumber=38932</a>> which is a software process assessment standard. Capability-level names are adopted from that standard. The new levels for the capability and maturity model are

- 0 Incomplete Process
- 1 Performed Process
- 2 Managed Process
- 3 Established Process
- 4 Predictable Process
- 5 –Optimizing Process

#### 6. Goals Cascade

CobiT 5 provides a link between stakeholders' expectations and practical goals providing more specific details. IT goals are derived from enterprise business goals, which in turn are derived from stakeholder expectations and values. This goal linkage is represented as a goal cascade in 5.0.

### 7. Enablers

CobiT 5 has seven categories of interrelated enablers and is driven by the goal cascade. The seven enablers for achieving enterprise goals are

- Processes
- Principles and Policies
- Organization structure
- Skills
- Culture
- Service Capability (from ITIL v3) and
- Information.

### 8. Control Objectives

Unlike the 210 control objectives in CobiT 4.1, there is no separate mention of control objectives in 5.0; such objectives are part of 208 management and governance practices. CobiT 5.0 is driven by stakeholder needs and not primarily by best practices.

### **SUMMARY OF CHANGES**

The following table summarizes the significant differences between CobiT 4.1 and CobiT 5.0.

Section	Parameter	CobiT 4.1	CobiT 5.0	
1	Driver	Best Practices	Stakeholder Expectations & Value	
2	Domains Areas	4 Domain Areas	5 Domain Areas. Though domain names are different they align with the domains in 4.1	
3	Process Areas	34 Processes	36 Processes	
4	Framework	Only CobiT 4.1 Framework	Integrated framework – Val IT, Risk IT, ITAF, BMIS etc. with CobiT 4.1	
5	Capability / Maturity Model	Maturity Model	Process Capability Model	
	Goals Cascade	IT goals are derived from business goals of maintaining enterprise reputation and leadership	IT goals are derived from stakeholders needs and expectations	
6	Enablers	No mention of Enablers	Identified 7 Enablers	
7	Control Objectives	210 Control Objectives	No separate mention of control objectives but included as part of	

Management and Governance	
Practices	

#### **IMPLEMENTING CobiT 5.0**

It will be easier for an organization to start fresh with 5.0 than to transition from 4.1. Rebuilding the entire IT governance structure may be easier and more cost effective if an organization is at maturity level 2 or below, where processes are ad hoc, undefined and undocumented.

However, if an organization has heavily invested in 4.1 initiatives, they can align to 5.0 later after or arriving at a logical closure point. They can still leverage existing 4.1 documents with certain modifications to satisfy 5.0 requirements. The main difference will be to structure the processes from 4.1 into the governance and management domain.

CobiT 5.0 is comprehensive and voluminous; each organization should use relevant portions and customize to meet their specific objectives based on stakeholder needs and expectations.

CobiT 5.0 will make significant contributions to enterprise governance. With proper transition planning, the overall costs to the organization should be minimal and the benefits of great value.

\* \* \*

Pritam Bankar< <a href="http://www.linkedin.com/in/pritambankar">http://www.linkedin.com/in/pritambankar</a> >, CISA, CISM is solution lead at Infosys< <a href="http://www.infosys.com">http://www.infosys.com</a> >, a leading infrastructure security & compliance practice. He has more than eight years of experience and has led several IT strategy consulting engagements in the areas of information security, audits, compliance & regulations and IT Governance. Pritam has been a regular presenter at thought-leadership conferences and his articles are published in various information-security journals. He is also an active member of Cloud Control Matrix at Cloud Security Alliance<a href="https://cloudsecurityalliance.org/research/ccm/">https://cloudsecurityalliance.org/research/ccm/</a> > forum and ISACA. Pritam holds a Master's degree in information systems in addition to a Bachelor's degree in engineering from Mumbai University<<a href="https://www.mu.ac.in/">http://www.mu.ac.in/</a> >, India.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2012 Pritam Bankar & M. E. Kabay. All rights reserved.

## **Employment Practices & Policies**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Because people execute security policies (or violate them), hiring, managing and (alas) firing are important aspects of information assurance (IA) management. In a recent class discussion of personnel policies and security, the IS342 Management of Information Assurance<
<a href="http://www.mekabay.com/courses/academic/norwich/is342/index.htm">http://www.mekabay.com/courses/academic/norwich/is342/index.htm</a> > class reviewed some of the fundamental principles of personnel and security.

To start with, we face two fundamental problems in all discussions of crime, especially whitecollar crime, and particularly computer crime: we have incomplete ascertainment and we have incomplete reporting.

The problem of ascertainment lies in the difficulty of identifying crimes or errors that compromise confidentiality and control, at least until the malefactors reveal the data leakage by using the purloined information. And unfortunately, we don't yet have any centralized reporting of computer crimes or legal requirements for contributions to such a central database – so we lack reliable estimates of the frequency and severity of computer security breaches.

Nonetheless, a broad consensus among IA practitioners does support the belief that a sizable proportion of damage to computer systems may be from errors and omissions – perhaps even half. The attacks from the outside of systems and networks have increased over the last two decades because of the huge increase in interconnectivity due to wide use of the Internet.

Under these conditions, selecting appropriate employees can be a major contribution to effective IA. This review looks at hiring, management and firing from the perspective of IA managers.

### Hiring

Everyone with access to organizational information must be trustworthy; furthermore, it makes sense to put extra care into the hiring process for all employees who will be supporting computer systems such as operators, technical support personnel, programmers, managers, and security officers.

A degree of background checking is appropriate, but must respect applicable laws against discrimination in hiring. With the permission of the candidate, one can look for criminal records, and credit records as well as verifying claims of educational attainment and professional experience. Don't expect former employers to reveal much detail about the candidate beyond the dates of her employment; organizations are now highly sensitive to the risk of violating privacy laws or of stumbling into lawsuits for defamation.

In my experience as a technical services director for a sizable computer services company

several decades ago, I found it particularly helpful to have candidates for a particular job be interviewed by the staff currently involved in that kind of work. The staff can gently probe the candidates' bona fides with more detailed knowledge of the work that will be required than a manager who is a some remove from the day-to-day details of a job. They can also spot frauds more easily through their questioning; I remember one case where a poor fellow claimed to have three years of experience on the HP3000 (a "minicomputer" – think a big server) popular in the 1980s yet who could not log on to the system!

During the hiring process, successful candidates must be thoroughly briefed on corporate policies such as non-disclosure agreements for intellectual property, compliance with all regulations, and penalties for non-compliance. Some organizations have found it helpful to have a simple examination (usually automated) for the candidate to demonstrate knowledge of applicable policies.

### **Management**

One of the key attributes of successful security officers is the ability to assume an attitude of paranoia. You don't have to be paranoid: you just have to be able to act paranoid. Analysing how employees might abuse security systems and regulations is a constructive exercise in critical thinking. Security teams can benefit from exercises in thinking through how abuses could be carried out, how to respond, and how to improve processes to reduce risk. The organization should foster a belief in continuous process improvement, with suggestions for improvement welcomed, not criticized, and perhaps even rewarded. In one of my client sites, a factory, I remember seeing a poster that showed one of the employees with a big check – literally big: it was a couple of feet wide – made out for C\$25,000. That amount (even more impressive than today in 1983) was 10% of the savings the employee had fostered in the first year through a suggestion for modifications in the production environment.

Another critical tool in training employees is how to respond to attempted collusion. An employee can practice dealing with such an uncomfortable situation in training sessions to get used to the idea that the first response should be to appear interested; the second is to report the attempted collusion to management so they can decide on appropriate actions (e.g., create a sting operation, record interactions with the criminal, and contact law enforcement).

One of the principles I teach is that access to computer systems or information is a privilege, not a right. It is unwise to grant access privileges to managers who don't need it – there's a risk that access will become a status symbol instead of a privilege tied to specific job requirements. One of the incidents that I recall with amusement occurred around 1985 when the president of the company I worked for brought a visitor from Toronto to our Montreal data centre on a Saturday night and asked the operator to let them into the computer operations room. The operator politely refused because the president was not on the list of approved unaccompanied visitors. The young man offered to call me for permission, but the president took the snub in good spirits. Indeed, he wrote a letter of commendation for the operator a couple of days later.

Another principle is "Kabay's Law:" NO ONE SHALL BE THE SOLE REPOSITORY OF CRITICAL INFORMATION OR SKILLS. There was a horrible example of the consequences of violating this principle in a case I was involved in the mid-1990s. A network administrator for the three offices of a law firm was increasingly erratic in his behaviour – and we consultants had

to meet offsite because there was reason to believe that he was reading all the e-mail of the executives! He was the only person who knew the root-access password, and he had never documented it in a way that his colleagues could have accessed. Dealing with an indispensable employee can be difficult. The norm must be that all operationally significant information must be documented; appropriate security for such documentation can include sealing passwords into opaque envelopes stored in the organization's safe and accessible when two high-placed executives sign for it. Periodic testing of such repositories is appropriate.

On the procedural side, everything that affects the mission-critical operations of the organization must be part of the institutional knowledge of the group. At least two people should always be able to accomplish any given critical task; they don't have to be perfect at it, but the disappearance of the prime should not put the organization in jeopardy.

Another guide for managers is to enforce vacations. There are two reasons for insisting on vacations. First, vacations offer an opportunity for live testing of the principles of operational resilience described above. Second, vacations offer an opportunity to see if someone has been carrying out secret operations that must be continued to avoid discovery. For example, if an accountant has been embezzling money by paying fake companies for non-existent services or goods (and using the fake bank accounts for his own benefit), a two-week absence may reveal the crime when another employee notices the fake entries and investigates what they were supposedly for.

If employees change their interpersonal style radically – whether for good or ill – supervisors might want to look into the situation. Becoming friendly (or angry, or depressed) does not mean necessarily that an employee is involved in anything bad, but managers will do well to investigate. I remember one astounding case where a modestly paid employee showed up at work with an expensive new car and claimed he had won a lottery. However, there was no public record of his winning anything – but investigation of his work showed that we was involved in taking bribes for relaying sensitive information.

The principle of separation of duties means that no critical operation should be completed by a single person. In the embezzlement scenario, it was a problem that the accountant was able to create invoices, approve them, and pay them without supervision.

Another warning for employers is that security policies must absolutely forbid unauthorized security testing. There have been many cases in which well-meaning employees have been fired for foolishly testing system security without informing anyone in advance and obtaining written authorization by a suitable manager. And on the converse side, claiming good intentions for security probes may be a cover for nefarious plans.

### **Termination of Employment**

Well, things haven't gone as well as they should. One or more employees must be fired for reasons such as workforce reductions, mergers and acquisitions, or inadequate individual performance. The basic rule is that absolutely everyone must be treated with the same procedure and the same respect, regardless of manager's emotions about the termination. If Albert is frogmarched to the exit by a security guard whereas Betty is treated to a joyful party, the message is clear: Albert is bad and Betty is good. Such implicit criticism and praise can lead to lawsuits for defamation (by the Alberts). It is best to maintain strict even-handedness when firing people;

then the employees can organize a farewell party privately, on their own time, off the organization's premises.

What about resignations? What is old Charlie has worked diligently for 30 years and is beloved by all? Can't we have a farewell party on the organization's premises? Well, it's a pity, but in a litigious environment, it's best to have the party off premises. Now, Charlie probably let people know about his pending resignation months or years before the event (for example, I have already told my Dean to expect my resignation at the end of May 2025), so there is no need for any surprise in how he is treated. Furthermore, it may be valuable for Charlie to help document details of his work that may not have made it into institutional knowledge and to train his replacements. Nonetheless, exactly the same process as for anyone else would apply to Charlie on the last day of work – the exit interview, clearing the desk, returning identification cards, and returning other corporate property.

An exit interview can be either a painful exercise or a positive experience. If the separation is amicable, the departing employee may be able to contribute insights that might have been more difficult to impart to managers while she was employed. Even if there is some friction underlying the departure, it's still possible to extract useful information from the employee if she is willing to speak her mind.

Finally, the termination process must be tightly coordinated between the human resources group and the information technology and IA group. As the exit interview is underway, the employee's access privileges must all be revoked and assigned to appropriate replacement personnel who will take up the tasks of their former colleague.

For a more detailed version of these points, you can see Chapter 45, "Employment Practices & Policies" by myself and Bridgett Robertson in the *Computer Security Handbook*, 5<sup>th</sup> edition.<a href="http://www.amazon.com/Computer-Security-Handbook-Volume-Set/dp/0471716529/">http://www.amazon.com/Computer-Security-Handbook-Volume-Set/dp/0471716529/</a>. For a PowerPoint presentation on the subject, you can freely download a PPTX<a href="http://www.mekabay.com/courses/academic/norwich/is342/is342">http://www.mekabay.com/courses/academic/norwich/is342/is342</a> lectures/csh5 ch45 employment practices policies.pdf > version of the lecture notes.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:mekabay@gmail.com">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2012 M. E. Kabay. All rights reserved.

# Terrifying Your Employees: Not Recommended for Training

### By Michael Krausz, & M. E. Kabay, PhD, CISSP-ISSMP

The following contribution is from information security expert Michael Krausz in Vienna with editorial and textual contributions from Mich Kabay.

At a courthouse in Austria, on 28 February 2012, a security-training exercise went wrong.

In the weeks running up to the events of 28 February, police forces and the courthouse management were involved in planning what they believed to be a bright idea: conducting an exercise for courthouse staff on how to respond to someone running amok within the building.

Such an incident had happened only a couple of months before at a different courthouse in a different state in Austria, leaving two people dead (including the perpetrator) and a number of staff severely traumatized.< <a href="http://derstandard.at/1330389968074/Klagenfurt-Amoklaufuebung-am-Gericht-Mitarbeiter-unter-Schock">http://derstandard.at/1330389968074/Klagenfurt-Amoklaufuebung-am-Gericht-Mitarbeiter-unter-Schock</a>>

Training for such an event, by itself, was therefore not a bad idea, although such events are extremely rare in Austria (this was second such incident in about 50 years).

The exercise was executed on 28 February by police forces and conducted in an extremely realistic way. Realistic indeed: it included one simulated death, apparently by a gunshot to the head. Makeup was used to simulate injuries, and several officers were placed in the building as if they were injured persons. The supposed death was staged in front of courthouse staff who were evacuating offices.

There was one catch, though: the exercise was entirely unannounced to staff and no preparations whatsoever were taken to prepare staff for the experience.

The effect of this omission was devastating. By the next day 40 staff members were in treatment for severe trauma and an undisclosed number had taken sick leave. We must assume that some will suffer from post-traumatic stress disorder (PTSD) in the weeks and months to come.

In a TV interview, a courthouse spokesperson justified actions by stating that the exercise was unannounced because "...[I]t is our experience that announced exercises are not taken seriously by staff." Although this assertion may be true, it does not justify exposing staff to a potentially traumatizing experience, especially given that if people cannot determine if a situation is staged or real, they must assume that it is real.

As this is being written (mid-March 2012), the latest news about the botched training exercise is that affected staff members still receive treatment and the next in line superior court to the one affected has publicly apologized for the exercise.

http://derstandard.at/1330390059483/Klagenfurt-Amokuebung-am-Gericht-Justiz-entschuldigt-sich >

For all of us planning awareness and training, it is essential to remember that surprising, frightening, embarrassing and humiliating our colleagues will not help improve security. There is no point in going through the expense of simulations and tests if we have not prepared our teams effectively and resolved everything that can be resolved before the exercises. Having unprepared staff members also means that no one is monitoring events dispassionately – or with video footage – for an effective post-training discussion of what can be improved. Exercises are supposed to contribute to continuous process improvement, not nightmares.

We finish with sound advice from noted security expert and author Rebecca Gurley Bace < <a href="http://www.infidel.net/page1/page2/">http://www.infidel.net/page1/page2/</a> > wrote in her chapter (#46) of vulnerability assessment (VA) in the *Computer Security Handbook*, 5<sup>th</sup> Edition</a> <a href="http://www.amazon.com/Computer-Security-Handbook-Volume-Set/dp/0471716529/">http://www.amazon.com/Computer-Security-Handbook-Volume-Set/dp/0471716529/</a> >,

Given the relatively unconstrained spirit associated with penetration testing, it is critical that the process be managed properly. Some of the requisite management considerations mirror those of the more generic process of [vulnerability assessment (VA)]. Independent oversight is required for the conduct of VA; it is especially critical to the success of penetration testing. Test scenarios should be documented and approved in advance by at least two representatives of the organization being tested, and the employees of the organization should be prepared for testing, especially when social engineering techniques are included in the scope of penetration testing.

This set of agreements and preparation for testing is key to balancing the need to perform realistic and relevant VA (including penetration testing) with the need to minimize the impact of such testing on normal business operations.

As human systems and constructs are as much a part of business operations as information systems, minimizing impact involves consideration of the ethics of social engineering. The first ethical tenet asserts that social engineering tests should not cause psychological distress to test subjects. Most employees are conscientious with regard to security and other company policies and may consider being targeted by social engineering tests as a breach of trust. Their reactions to that perceived breach may range from anger to resignation, or to a lawsuit.

Another ethical tenet states that those who fail social engineering or other penetration tests should not be subject to humiliation; this requires that test results be treated as confidential information. Finally, testers should not rely unduly on verbal misrepresentation or acting to achieve the goals of testing—the objective of such testing is to establish whether security measures are appropriate and effective for the organization, not to score a win for the test team at all costs. To leave a tested organization in worse condition than the test team found it is a hollow victory for all involved.

So forget dreams of Hollywood special effects and a compelling theatre experience: involve employees in all preparations for exercises, drills, simulations and tests.

\* \* \*

Michael Krausz studied physics, computer science and law in university. He is a professional investigator as well as lead auditor for ISO27001 compliance. He designed the first ever information security training classes in Austria (1998) and has assisted in setting up certifying bodies and accreditation authorities for ISO27001/ISO27006. Having worked in 14 countries so far on a range of information security topics, Mr. Krausz has published two Englishlanguage books on managing information security breaches [*Information Security Breaches: Avoidance and Treatment Based on ISO27001 < http://www.amazon.com/Information-Security-Breaches-Avoidance-Treatment/dp/1849280274/ > & Managing Information Security Breaches < http://www.amazon.com/Managing-Information-Security-Breaches-*

Michael/dp/1849280940/ >]. He has recently published a German-language book on the dangers and challenges the Internet for the individual and the state in collaboration with the head of the Cybercrime Unit at the Austrian Federal Criminal Intelligence Agency, Mr. Leo Löschl [Schauplatz Cyberworld, < http://www.amazon.de/Schauplatz-Cyberworld-Leopold-L%C3%B6schl/dp/3902494557/ref=sr\_1\_1?ie=UTF8&qid=1332099651&sr=8-1>]. Mr. Krausz is a national member of ISO's JTC1/SC27/WG1 committee and editor of ASIS's investigation council's newsletter.

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

Copyright © 2012 Michael Krausz & M. E. Kabay. All rights reserved.

## **Sharing Security Information for International Peace**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

It's a commonplace that information assurance suffers from two fundamental problems in information acquisition: failure of ascertainment (failing to realize that a breach of security has occurred) and failure of reporting (keeping apprehend breaches secret). In an overview of statistical methods in computer-crime reporting<

http://www.mekabay.com/methodology/crime\_stats\_methods.pdf >, I pointed out that one of the most striking research studies of ascertainment and reporting was carried out by the United States (US) Department of Defense:

In a landmark series of tests at the Department of Defense, the Defense Information Systems Agency found that very few of the penetrations it engineered against unclassified systems within the DoD seem to have been detected by system managers. These studies were carried out from 1994 through 1996 and attacked 68,000 systems. About two-thirds of the attacks succeeded; however, only 4% of these attacks were detected.... [O]f the few penetrations detected, only a fraction of 1% were reported to appropriate authorities.

One interpretation at the time was that if the US military was incapable of convincing its professionals to notice and report more than a tiny fraction of the minority of penetrations that were even noticed, the chances were low that non-military branches of the government, private industry, and other non-governmental organizations were doing even that badly.

One of the reports on this project is in the "Security in Cyberspace" document presented to the Permanent Subcommittee on Investigations of the Committee on Governmental Affairs of the United States Senate for the 104th Congress, on May 22, June 5, 25 July & July 16, 1996. Several formats of the report are available online <

http://archive.org/details/securityincybers00unit > including the 29MB PDF version.< http://archive.org/download/securityincybers00unit/securityincybers00unit.pdf >. There is a reference to the 65% successful penetration rate on page 37 of that document.

### US Government Projects

There has been progress in information sharing about computer crime. For example, the Common Vulnerabilities and Exposures (CVE< <a href="http://cve.mitre.org/">http://cve.mitre.org/</a>) Database run for the US government's Computer Emergency Readiness Team< <a href="http://www.us-cert.gov/">http://www.us-cert.gov/</a>> of the National Cyber Security Division</a> <a href="http://www.dhs.gov/xabout/structure/editorial\_0839.shtm">http://www.dhs.gov/xabout/structure/editorial\_0839.shtm</a>> in the Department of Homeland Security(DHS</a> <a href="http://www.dhs.gov/index.shtm">http://www.mitre.org/about/</a> has been widely adopted</a> <a href="http://cve.mitre.org/compatible/index.html">http://cve.mitre.org/compatible/index.html</a> by organizations around the world as a repository of shared definitions and descriptions of what it defines as follows: "An information security 'vulnerability' is a mistake in software that can be directly used by a hacker to gain access to a system or network." These definitions provide a basis for information sharing by standardizing terminology so that different software systems and databases can share data using the same

nomenclature. Even if internal names used within the different products don't match, tables of equivalence of the local names with CVE entries can still allow communications.

To search the CVE, use the National Vulnerability Database<
http://web.nvd.nist.gov/view/vuln/search-results?query=&search\_type=all&cves=on >
maintained by the National Institute of Standards and Technology (NIST). At the time of writing
(mid-March 2012) there were 49,627 records in the database.

Another constructive US government contribution to security-information sharing is the "Information Sharing Strategy for the Department of Homeland Security" (ISS< <a href="http://www.dhs.gov/xlibrary/assets/dhs\_information\_sharing\_strategy.pdf">http://www.dhs.gov/xlibrary/assets/dhs\_information\_sharing\_strategy.pdf</a> >) of 2008. The DHS summarized the strategy as follows:

The President and Congress have directed the DHS to perform an essential and multi-faceted mission: prevent and protect against terrorist attacks; respond to both man-made and natural disasters; perform the law enforcement and other crucial functions of the Department's component agencies; and play a central role in augmenting the Nation's ability to gather, analyze and disseminate information and intelligence.

To ensure that information and intelligence flow where and when they should, DHS must foster information sharing, consistent with law, regulation and policy, in each of the following ways: i) internally within DHS, ii) horizontally within the U.S. government between both law enforcement agencies and the intelligence community, iii) vertically with State, local, territorial, tribal and private sector partners, and iv) horizontally with the law enforcement and intelligence agencies of foreign allies and appropriate international institutions.< <a href="http://ise.gov/mission-partners/department-homeland-security">http://ise.gov/mission-partners/department-homeland-security</a>

The ISS established Information Sharing Standards described as follows (summarizing p.7):

- Functionality in the critical infrastructure is primary, not technological details;
- Information sharing will maximize interoperability regardless of technical infrastructure;
- Readily-available commercial standards and protocols will be the standard for information interchange;
- Information sharing will respect privacy and security of the shared data.

The overview page< <a href="http://www.dhs.gov/files/programs/sharing-information.shtm">http://www.dhs.gov/files/programs/sharing-information.shtm</a> > for information-sharing projects run by DHS includes details and links for three computer-related services among the nine listed:

- Automated Critical Asset Management System (ACAMS
   <a href="http://www.dhs.gov/files/programs/gc\_1190729724456.shtm">http://www.dhs.gov/files/programs/gc\_1190729724456.shtm</a>>)
- CIKR Asset Protection Technical Assistance Program (CAPTAP
   <a href="http://www.dhs.gov/files/programs/gc\_1195679577314.shtm">http://www.dhs.gov/files/programs/gc\_1195679577314.shtm</a>>)
- Protected Critical Infrastructure Information (PCII
   http://www.dhs.gov/files/programs/editorial\_0404.shtm >) Program

### UK & EC Programs

In the United Kingdom (UK), plans released in November 2011 for a UK cyber-security and cyber-crime strategy include a special unit with the National Crime Agency<

http://www.homeoffice.gov.uk/crime/nca/ >. Writing for eWeek <a href="http://www.eweek.com/c/a/Security/UK-CyberSecurity-Strategy-Beefs-Up-Defenses-Information-Sharing-409924/">http://www.eweek.com/c/a/Security/UK-CyberSecurity-Strategy-Beefs-Up-Defenses-Information-Sharing-409924/</a>, Fahmida Y. Rashid added that

The plan outlined a new public-private sector collaboration in which the government and businesses will exchange information on cyber-threats and responses.... [T]he partnership will allow organizations to receive classified details about cyber-attacks and information on how to counter them."

Rashid writes that the definition of national infrastructure will be expanded to include more of the private sector, and the public will have a centralized system for reporting cybercrimes and receiving technical advice on appropriate responses.

At the European Community (EC) level, a report by Tom Espiner in ZDNet< http://www.zdnet.co.uk/news/security-threats/2011/12/07/certs-hindered-by-lack-of-sharingsays-eu-agency-40094599/ > discussed a report< http://www.enisa.europa.eu/act/cert/support/proactive-detection/ > by the European Network and Information Security Agency (ENISA) that failure to share information about cyber-incidents among national computer emergency response teams (CERTs) is reducing the effectiveness of the organizations. ENISA published its report in English< http://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detectionreport/at download/fullReport > and also a summary of the survey< http://www.enisa.europa.eu/activities/cert/support/proactive-detection/proactive-detection-report > that was used in preparing the full report. The report describes and evaluates 30 different "Services for the proactive detection of network security incidents" (p 27 ff using the page numbers in the document, not the PDF page numbers) and 12 "Tools/mechanisms for the proactive detection of network security incidents" (p75 ff). The report continues with detailed analysis of "shortcomings in the proactive detection of incidents" (p 108 ff) and ends with several pages of recommendations (p 128 ff) for both data providers and for data consumers. The conclusions (p 133) end with the assertion about the importance of data sharing: "The end goal is improving data sharing and cooperation in proactive detection and incident handling between CERTs – an essential element for the successful mitigation of cyber-attacks."

#### Private Sector

Internationally, organizations such as SANS< <a href="http://www.sans.org/">http://www.sans.org/</a> > do their best to share security information using "Consensus Research Projects" which currently include the following three relevant titles:

- 20 Critical Security Controls < http://www.sans.org/critical-security-controls/ >
- Top Cyber Security Risks < http://www.sans.org/top-cyber-security-risks/ >
- Top 25 Software Errors < http://www.sans.org/top25-software-errors/ >

Among the countless research scientists constantly publishing valuable insights into systemic and specific errors in security and recommending practical improvements, Peter G. Neumann<a href="http://www.csl.sri.com/users/neumann/">http://www.csl.sri.com/users/neumann/</a> >, Principal Scientist for the SRI International Computer Science Laboratory < <a href="http://www.csl.sri.com/">http://www.csl.sri.com/</a> > is one of the stars of the academic firmament. He has been moderating the "Forum on Risks to the Public in Computers and Related Systems" (usually just called the *Risks Digest* <a href="http://catless.ncl.ac.uk/Risks/">http://catless.ncl.ac.uk/Risks/</a> >) continuously, brilliantly and amusingly (he is an inveterate punster) since 1985. As a contribution to ease of access, I

have compiled PDF files< <a href="http://www.mekabay.com/overviews/risks/index.htm">http://www.mekabay.com/overviews/risks/index.htm</a> for each volume from 1 to 25 (1985-2010) and will be adding the next volumes within a few months of this writing. Readers may also download a single ZIP archive<
a href="http://www.mekabay.com/overviews/risks/risks">http://www.mekabay.com/overviews/risks/risks</a> 01-25 pdf.zip > file with all the PDF files for volumes 1 to 25 and another ZIP archive<
a href="http://www.mekabay.com/overviews/risks/risks">http://www.mekabay.com/overviews/risks/risks</a> 01-25 pdx.zip > with PDF index (PDX) files for rapid local lookup.

### **Concluding Remarks**

I want to finish with a few personal comments about how I see the international implications of data sharing to fight cyberattacks and rectify vulnerabilities.

Criminals and terrorists worldwide now have the power to engage in asymmetric warfare against the critical infrastructure of nation-states. A few people can create and control botnets<
http://www.honeynet.org/papers/bots/ > involving thousands of compromised systems that can spread malware and launch distributed denial-of-service attacks that can impede access to or even crash targeted production systems. Tailored malware such as Stuxnet<
http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1 > can target specific models and brands of supervisory control and data acquisition (SCADA) systems. Volunteer hacktivists can reveal vast volumes of classified materials< http://wikileaks.org/ >, with unpredictable effects on public reaction, government policy, and international diplomacy. Such electronic gangs may even be out-stealing<
http://www.wired.com/threatlevel/2012/03/hacktivists-beat-cybercriminals/ > cybercriminals. And state-sponsored actors could easily carry out attacks on a particular target using IP-spoofing</h>
http://www.sans.org/reading\_room/whitepapers/threats/introduction-ip-spoofing\_959 > to divert attention from their country to some other target in the hope of provoking international conflict.

As the reliance on information systems in critical infrastructure has increased over the last several decades, the need for information sharing has grown not only to increase technical resistance to failures and to attacks: information sharing has become essential to prevent international conflicts based on the behaviour of non-state actors, on misunderstandings, and on deliberate sabotage and misrepresentation. Effective information sharing, especially between and among potential adversaries, may be a tool for increasing cooperation and reducing hostility on the international stage.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:mekabay@gmail.com">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2012 M. E. Kabay. All rights reserved.

# Vulnerability Management is Essential for Effective Security

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Vulnerability management is the embodiment of continuous process improvement in system security.

In a recent discussion in the Norwich University< <a href="http://norwich.edu/">http://norwich.edu/</a> > IS342 (Management of Information Assurance< <a href="http://www.mekabay.com/courses/academic/norwich/is342/index.htm">http://www.mekabay.com/courses/academic/norwich/is342/index.htm</a> >) course in the Bachelor of Science in Computer Security and Information Assurance< <a href="http://programs.norwich.edu/business/csia/">http://programs.norwich.edu/business/csia/</a> >, the class reviewed Rebecca Gurley Bace's< <a href="http://www.infidel.net/bios/bacebio.php">http://www.infidel.net/bios/bacebio.php</a> > chapter 46, "Vulnerability Assessment" from the <a href="http://www.amazon.com/Computer-Security-Handbook-Volume-Set/dp/0471716529/">http://www.amazon.com/Computer-Security-Handbook-Volume-Set/dp/0471716529/</a> >.

Bace explains that vulnerability management includes several phases:

- Assessing deployed information systems to determine their security status;
- Determining corrective measures
- Managing the appropriate application of the corrections.

The four basic functions of vulnerability management are

- Inventory: identify all systems in the domain of interest, including operating systems, platforms, and topology;
- Focus: determine the data required for assessment and tune vulnerability-assessment tools;
- Assess: run automated and manual tests, evaluate results to judge risk to the systems using security policy and best practices;
- Respond: execute changes as required by assessment and fix specific weaknesses.

Vulnerability assessment (VA) involves gathering sample data, organizing the data, comparing the current status with reference standards, and identifying discrepancies between the current state and recommended standards or goals. An example of a well-known VA tool is the Microsoft Baseline Security Analyzer v2.2 (MBSA<

http://www.microsoft.com/download/en/details.aspx?id=7558 >) that "provides a streamlined method to identify missing security updates and common security misconfigurations." The product has been updated over the years to support Windows 7 (32- and 64-bit) and Windows Server 2008 R2 as well as older operating systems back to Windows XP and Windows 2000. It also looks for documented weaknesses in "all versions of... Internet Information Server (IIS) 5.0, 6.0 and 6.1, SQL Server 2000 and 2005, Internet Explorer (IE) 5.01 and later, and Office 2000, 2002 and 2003 only." Versions of the human interface are available in German, French, and Japanese in addition to English.

For an excellent overview of how a well-design VA tool can support security management, see the extensive set of white papers< http://www.stillsecure.com/library/vam.php > from

StillSecure about their "VAM" product.

VA fits into security management in many ways:

- When systems are first deployed, VA can establish a baseline definition of the security state;
- When security breaches are suspected, VA users can focus on likely attack paths;
- VA may help administrators to see if vulnerabilities have been exploited;
- VA can identify areas where newly reported vulnerabilities should be patched;
- Records of VA scans can be archived and serve for audits or for compliance with certifications.

At a fundamental level, VA systems support *auditability*, which in turn supports incident handling and recovery. VA is an essential part of continuous process improvement for security policies to adapt to the constantly changing threat-and-vulnerability environment.

### **History and Directory of VA Tools**

One of the earliest VA tools was COPS<

<u>ftp://ftp.cerias.purdue.edu/pub/tools/unix/scanners/cops/</u> > (Computer Oracle and Password System) developed by Eugene "Spaf" Spafford< <u>http://spaf.cerias.purdue.edu/</u> > and Dan Farmer< <u>http://www.linkedin.com/in/zenfish</u> > at Purdue University.

In the early 1990s, the Internet Security Scanner (ISS) was the subject of a Computer Emergency Response Team Coordination Center (CERT-CC) Advisory < <a href="http://www.cert.org/advisories/CA-1993-14.html">http://www.cert.org/advisories/CA-1993-14.html</a> > warning of "software that allows automated scanning of TCP/IP networked computers for security vulnerabilities."

Dan Farmer & Wietse Venema< <a href="http://www.porcupine.org/wietse/">http://www.porcupine.org/satan/</a> (Security Administrator Tool for Analyzing Networks) in the early 1990s and posted the code in 1995. For an overview of the tool, see the page<a href="http://www.cerias.purdue.edu/about/history/coast/satan.php">http://www.cerias.purdue.edu/about/history/coast/satan.php</a> at the Center for Education and Research in Information Assurance and Security (CERIAS).

NESSUS< <a href="http://www.tenable.com/products/nessus">http://www.tenable.com/products/nessus</a> > from TENABLE Network Security is described by the company as "the world's most widely-deployed vulnerability and configuration assessment product with more than five million downloads to date." The product is freely available for individual, non-commercial use< <a href="http://www.tenable.com/products/nessus/nessus-homefeed">http://www.tenable.com/products/nessus/nessus-homefeed</a> > and has an evaluation version</a> <a href="http://www.tenable.com/products/nessus-professionalfeed/nessus-evaluation">http://www.tenable.com/products/nessus-professionalfeed/nessus-evaluation</a> > for use by organizations. The evaluation page includes a chart comparing features of the evaluation version and the professional version, which at the time of this writing (April 2012) costs U\$1,500 per year.

NMAP< <a href="http://nmap.org/">http://nmap.org/</a> (NetMAPper) is a widely used freeware "for Linux, Windows, and Mac OS X." The home page boasts that "Nmap was named "Security Product of the Year" by Linux Journal, Info World, Linux Questions. Org, and Codetalker Digest. It was even featured in eight movies, including *The Matrix Reloaded*, *Die Hard 4*, and *The Bourne Ultimatum*." [Perhaps other products should consider demonstrating their quality by appearing in popular

movies. Imagine how popular MS Word could become if it appeared in Monty Python movies!]

One of the most useful tools for individual users as well as for network administrators is Steve Gibson's ShieldsUP! service< <a href="https://www.grc.com/x/ne.dll?bh0bkyd2">https://www.grc.com/x/ne.dll?bh0bkyd2</a> > which provides a quick scan of the first 1056 ports of an individual computer. Ideally, every port will register as "Stealth" (not responding to probes) or at least as "Closed" (not accepting connections).

For links to more products, see the excellent "Alphabetical List of Vulnerability Assessment Products" < <a href="http://www.timberlinetechnologies.com/products/vulnerability.html">http://www.timberlinetechnologies.com/products/vulnerability.html</a> > maintained by Timeberline Technologies</a> <a href="http://www.timberlinetechnologies.com/index.html">http://www.timberlinetechnologies.com/index.html</a> >.

### **Concluding Remarks**

One of the most important suggestions for effective penetration testing (pen testing) is that vulnerability analysis and vulnerability remediation must precede testing. It's pointless to waste time and money on pen testing if we haven't corrected everything we can find using scanners.

\* \* \*

For study notes on vulnerability assessment, download the IS342 PPTX<
http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch46\_vulnerability\_assessment.pptx > or PDF<
http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch46\_vulnerability\_lectures/csh5\_c

ity\_assessment.pdf > files.

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

Copyright © 2012 M. E. Kabay. All rights reserved.

# **Reality Trumps Theory**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

A local reporter spent eight hours interviewing students and faculty in the computer science <a href="http://programs.norwich.edu/business/computerscience/">http://programs.norwich.edu/business/csia/</a> > programs at Norwich University <a href="http://www.norwich.edu">http://www.norwich.edu</a> > a couple of days before I began writing this article. At one point, he asked half a dozen of our students what they felt was special about their education in the School of Business and Management <a href="http://programs.norwich.edu/business/fac-bus/">http://programs.norwich.edu/business/fac-bus/</a> >. One young man responded immediately that the focus in our programs is service to organizations in furtherance of their mission-critical objectives; in contrast, he said, he had the impression that some of the students he had met from well-established programs at other institutions participating in various computing and security competitions were focused primarily on details of technology. "People use technology to achieve business goals," he said, "not just because technology is interesting and fun." Another student laughed and pointed at me: "Prof Kabay has drilled us in every course with his motto, 'Reality trumps theory." Students nodded and explained that they had learned never to solve problems by applying rote learning as if recipes and checklists could be applied without careful consideration of the specific requirements of any situation.

I was delighted to see that my brainwashing, er, education in principles was having such an effect on our students. The phrase "Reality trumps theory" became the motto for the master's program in IA< <a href="http://infoassurance.norwich.edu/">http://infoassurance.norwich.edu/</a> that I designed and helped to establish in 2002. As the students correctly explained, I have a deep suspicion about absolute rules divorced from the particular details of the problem confronting us. For example, one can easily find a perfectly good principle being turned into rigid dogma; consider "Change your password frequently." I have encountered organizations where the IA or IT staff have dictated monthly changes in logon passwords despite the consequences: employees either chose a ridiculously simple, easy-to-guess passwords or they wrote down complex passwords on papers and stuck them in obvious places such as underneath their keyboard or inside a desk drawer. Bruce Schneier, in contrast (and as usual) takes a far more intelligent attitude to changing passwords.<a href="http://www.schneier.com/blog/archives/2010/11/changing\_passwo.html">http://www.schneier.com/blog/archives/2010/11/changing\_passwo.html</a> > For example, he concludes his thoughtful review of the question with the following well-reasoned advice:

"So in general: you don't need to regularly change the password to your computer or online financial accounts (including the accounts at retail sites); definitely not for low-security accounts. You should change your corporate login password occasionally, and you need to take a good hard look at your friends, relatives, and paparazzi before deciding how often to change your Facebook password. But if you break up with someone you've shared a computer with, change them all."

What a contrast with "You must change your password every 30 days and that's all there is to it." The discussion at the end of the article includes many thoughtful postings from readers, most of whom seem to me would agree with the principle that "reality trumps theory."

IA is a balancing act: we must constantly weigh benefits against costs – and I'm not just talking about direct financial costs. Despite our heartfelt yearning for quantitative risk management, we are stymied by the lack of an adequate statistical base for annualized loss expectancies (ALE<
http://www.riskythinking.com/glossary/annualized\_loss\_expectancy.php >). We have neither accurate frequency data for specific problems nor accurate data about monetary losses. As I Have explained for decades< http://www.mekabay.com/methodology/crime\_stats\_methods.pdf >, information security breaches suffer from the problem of ascertainment (we may not notice a breach at all or not for long time) and the problem of reporting (we have no centralized data collection facility and victims may choose not to report breaches and costs to anyone). Using best practices and formal standards make sense, but no set of prescriptions can be applied as if we were following a recipe.

One of the resources in security-policy development I have used since the 1980s is the evolving series, "Information Security Policies Made Easy" by Charles Cresson Wood (ISPME< <a href="http://www.informationshield.com/ispmemain.htm">http://www.informationshield.com/ispmemain.htm</a> >). Now in its 12th edition, ISPME consistently emphasizes importance of adapting the recommended policies to the specific needs of the customer. I opened my copy of the 10th edition at random and immediately found the following example of Wood's emphasis on thoughtful application of policy rather than dogmatic rigidity:

#### 2. Performance Evaluations

Policy: Compliance with information security policies and procedures must be considered in all employee performance evaluations.

Commentary: This policy requires management, at the time they write performance evaluations, to decide whether the involved employee has been be concerned about information security, and if the answer is yes, then to determine whether the employee has acted in compliance with policies and procedures. The policy provided here makes direct reference to the management activity of evaluating employees, and only indirectly to a rank-and-file employee activity of complying with policies and procedures. Nonetheless, it implies that both are expected by management. The words "information security policies and procedures" could be changed to "information security requirements" or other generic terms used at the organization.

Related Policies: "Information Security Responsibility" and "Information Security Liaisons."

Audience: Management

Security Environments: All

In my career, I have been saddened to see IA being damaged by authoritarians who refuse to discuss policies with concerned users. These people act as if their primary goal is enforcement of their initial conception of appropriate security, impervious to warnings that their initial conception is wrong and uninterested in changing circumstances that render their absolute rulings ineffective by any standard. These autocrats enrage their customers – and yes, I always use the concept that information technology and information assurance should consider the user community their customers – and result in widespread contravention of their inappropriate

policies.

In closing, I want to remind readers that one of the most effective tools for establishing well-received security policies is to explain the reasons behind every policy. Charles Cresson Wood has used this technique throughout his work, as exemplified in the commentaries for every suggestive policy in his magisterial text. When I ran my own consulting firm, the company's motto was "Progress Toward Autonomy" and I required every contract to include a specific person with whom I could discuss every step of the performance optimization, operations management restructuring, or security assessment for which I was being paid. In my teaching, every recommendation, every principle is explained, not dictated; I constantly urge my students not to memorize, but to integrate knowledge.

Life is not a computer game with rigid and predictable rules; life is a multidimensional manifold that changes all the time.

Reality trumps theory.

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

Copyright © 2012 M. E. Kabay. All rights reserved.

# **Prototyping in Real Life**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

In business continuity planning (BCP<

http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch58\_bcp.pdf >) and disaster recovery planning (DRP<

http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch59\_drp.pdf >, it's a commonplace to urge planners to create initial plans and then test them for ways to improve. This approach is parallel to the current standards of software development and risk management. In the 1960s and 1970s, the standard software development methodology was the system development life cycle (SDLC< <a href="http://www.waterfall-model.com/sdlc/">http://www.waterfall-model.com/sdlc/</a>>), in which analysis, design, and approvals of the complete design were so onerous that delivery of finished software could be delayed by years. Since the 1980s, a much more common methodology is spiral development</a> <a href="http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA382590">http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA382590</a>>, which was originally called rapid application development (RAD<

http://www.gantthead.com/content/processes/11306.cfm >), joint application development (JAD< http://www.umsl.edu/~sauterv/analysis/488\_f01\_papers/rottman.htm >), or iterative, agile and incremental development< http://www.craiglarman.com/wiki/downloads/misc/history-of-iterative-larman-and-basili-ieee-computer.pdf >.

Spiral development teaches us to incorporate the Pareto Principle<

http://betterexplained.com/articles/understanding-the-pareto-principle-the-8020-rule/ > (the 80/20 rule) into any project. If much of the desired result can be achieved with modest effort / resources / time, then it makes sense to get a first-cut version of any project in place before trying to refine it. Effective risk management takes advantage of incremental gains by instituting the best available defences and policies and then improving them; "lessons learned" is often used in after-incident reports (post mortems) on such systems. It would be ridiculous to have no defences or policies because they wouldn't be perfect.

When I proposed the Master of Science in Information Assurance <a href="http://infoassurance.norwich.edu/">http://infoassurance.norwich.edu/</a> > to the University Curriculum Committee at my university in 2002, I was astonished at the reaction of a humanities professor. He said that there was insufficient evidence from scholarly research to be able to judge the proposals, and therefore, the entire project should be delayed for at least a year as we provided the Committee with additional grounds for believing that the program would be successful. Luckily, I convinced the rest of the Committee that we would be revising the program constantly (continuous process improvement again) and would learn from experience.

And that's what we did: we accepted a first class of 15 students in September 2002 and have been revising and adapting ever since.

Recently I was thinking about how these principles from systems engineering and information assurance can be applied constructively to ordinary life. I was prompted by memories of a discussion with an old friend many years ago about taking care of his disabled daughter after he died. To my surprise, I had ended up using the principles described above in our discussion of

his will. I've changed identifying details in what follows to protect his survivors' privacy.

Bob, now deceased, was then a 95-year-old retired history professor from a Midwestern university. He and his 93-year-old wife Frannie had discovered that their daughter Judy, then in her sixties, suffered from a severe personality disorder that had put her on psychiatric disability from the state where she lived for many years. She could live by herself only with great difficulty.

In our discussion, I asked what measures had been put in place in Bob and Frannie's wills to ensure that Judy could be financially secure after her parents died. To my horror, Bob said that they were still thinking about it. They wondered how to insulate Judy from her own tendency to become obsessively committed to particular political causes; they thought that if she gained access to a lump sum of inheritance, there were good chances that she would impulsively give it away to her favourite political action group (she was particularly concerned with wildlife preservation) in an emergency. Bob and Frannie were also devoted supporters of good causes, but they worried that Judy would be destitute, with no provisions for her own well-being.

Bob emphasized how he and Frannie had been "thinking about" the problem for a decade but still had not decided on the "perfect solution." I was horrified. I insisted that as Voltaire wrote, the perfect is the enemy of the good; waiting until all possible objections and eventualities were resolved could result in never actually acting at all. Indeed, Bob and Frannie had not included any details about how to protect Judy against her own mental disabilities in their will because they did not want to offend her.

For example, in Bob and Frannie's case, it would have been a good idea to have a will in place assigning Judy a trust fund from which she could draw periodically (every month, maybe) under the control of an executor rather than allowing the inheritance to be delivered to her in a lump sum. With that safety-net in place, the parents could then work on improving the arrangements. But not having anything in place was asking for trouble.

And trouble there was.

Bob died in 1998 and Frannie, as is so common<

http://seattletimes.nwsource.com/html/health/2014154333\_widow08.html >, died shortly thereafter. They had never completed their will, so Judy inherited the estate in toto. When 2001's terrible events of 9/11 occurred in New York, she was so moved that she gave away the totality of her inheritance to help victims and their families – admirable and loving, but she was left to survive on a pittance from the state. She was eventually thrown out of her apartment because of a citation from the public health officers in her city when her landlord reported that her obsessive hoarding<a href="http://understanding\_ocd.tripod.com/index\_hoarding.html">http://understanding\_ocd.tripod.com/index\_hoarding.html</a> > had resulted in a dangerous situation – her apartment was crammed floor to ceiling and wall-to-wall with hundreds of disintegrating cardboard boxes full of old clothing, useless crockery, and ancient magazines. Apparently she had even dragged in a filthy, stinking, soiled mattress salvaged from a garbage pile "because it might be useful." She disappeared after the eviction and no one knows what happened to her or whether she is still alive.

The principles of spiral development apply not only to software engineering, business continuity planning, and disaster recovery: they can be helpful in any enterprise where we are developing something new or unique and cannot simply apply an existing model to meet our needs.

Don't let the quest for an illusory perfection ruin a perfectly good project. Get on with the best you can do and adapt. Remember: Reality Trumps Theory.

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

Copyright © 2012 M. E. Kabay. All rights reserved.

# Protecting the Fish Pond: Lessons in Information Security from the Back Yard

by Jan Buitron, MSIA, CISSP, MCSE & M. E. Kabay, PhD, CISSP-ISSMP

Former student, good friend and brilliant colleague Jan Buitron, MSIA, CISSP, MCSE tells us a whimsical tale with lessons for us in the security field. Everything that follows is Jan's work with minor edits by Mich.

It was a big project for a homeowner. My friend set out to design, dig and decorate a fish pond out in her back yard. She dug the pond by hand, with her mother directing her in how to construct up from the bottom depth and sculpt the sides of the pond. She went to local rock and building supply stores to find just the right rocks to decorate the pond's margins. Careful planning went into designing the plant-scaping of the pond. Shorter plants were set around the pond's edges and, since they wanted the pond to attract birds, they made especially sure that there was at least one shallow area where the local birds could bathe easily.

They deliberately built deep areas into the pond, because the winters in the area can be quite cold, with temperatures at freezing and below for weeks at a time. The pond owner wanted the fish to overwinter in the pond, so the deeper areas allowed a place for the fish to avoid the colder upper waters. The deepest areas measured between four and a half to five feet.

I was close by at the time and watched the project progress, from first shovelful to adding the finishing touches such as floating night lights and landscaping with carefully selected rocks and rosebushes. And I had the privilege of attending their first-ever "Pond Party" where everyone was invited to bring not a covered dish, but a live fish to add to the pond, for colour and population.

Once the project was complete, the pond was a centrepiece in the yard, a haven of life, sound and colour, with the soothing sound of the waterfall cascading into the pond and the bright flashes of orange, black and white from the goldfish and koi living in its waters.

But, even a backyard project like a fish pond would have benefitted from a risk assessment and the advice of an experienced pond builder who fully understood the risks and vulnerabilities of having a fish pond in the yard.

My friend knew the problems of having dogs in the area, since two of her acquaintances owned Labrador retrievers that loved to leap into the pond on sight. However, there were additional, unplanned risks that eventually surfaced just over four years later.

It was the long Fourth of July Weekend. My friend had taken her boyfriend and dog to go camping in the mountains; they left on Friday night. I lived in her house part-time, and had decided to stay in her house part of the weekend to keep an eye on the place, arriving on Saturday afternoon.

On Sunday, the next morning, I went into the kitchen shortly after seven o'clock a.m. to prepare a pot of coffee. As I leaned toward the window overlooking the pond, I saw a huge set of wings flapping slowly next to the pond. A massive great blue heron rose elegantly into the air and flew away. His wingspan was at least five feet. I was thrilled for half a second, but my thrill melted into abject horror when I realized that he had been actively pursuing the fish in the pond! Feeling a little queasy, I delayed going out to take a look at the pond, fearing what I would see and

knowing that I couldn't do anything if any fish were gone.

Finally, when I went to check the pond with a gnawing ache in the pit of my stomach, the only fish that appeared to be left in the pond were the two large koi named Midge and Matsui. If I have ever seen fish that look frightened, those two looked terrified. The koi are larger fish, so I surmised they might have survived more easily, due to their size. The smaller fish were gone, all of them. I was saddened for the entire day.

\* \* \*

From an information assurance prospective, the pond was built without a thorough risk assessment. While the original pond advisor had some great ideas, not all of the risks had been factored in when building the pond. A professional pond installer might have advised installing anti-heron fences, or motion-sensing water spray devices that scare cranes and herons away from fish ponds. (If one searches YouTube.com for videos about herons raiding fish ponds, there are some hilarious videos of failed fish pond protections. Apparently, herons regularly scope out an area for ponds and open water and are always ready to 'dive in' at an opportune moment.)

Thus, a pond-risk-assessor would have advised building the pond with more hardened, protective coves for fish to hide from predators. This all could have been arranged after a complete, knowledge-backed pond risk assessment.

This is how it should be in information technology. An information system should be evaluated up-front before build out. Experienced information assurance professionals should be called in to sit down with business and process owners, the systems should be evaluated regarding the most critical components and protected accordingly. And, as in our fish-pond example, system owners do not always have a full picture of the risks involved in operating an information system. Without a, ah, full-scale risk assessment, critical risks could be overlooked with disastrous results.

There was one inadvertent protection that my friend had that worked to shield the pond from previous heron attacks . . . her dog. The fact that the dog went outdoors and spent time around the pond was duly noted by the ever-watchful herons.

One last mention, about five weeks after the great blue heron visited my friend's pond, I got an excited phone call. My friend breathlessly told me that the goldfish had appeared in the pond! All of them!! Apparently experts at self-preservation, the goldfish and smaller fish had dived down to the deepest area in the pond (over four feet), and stayed there for over five weeks, waiting for the all clear. And sure enough, there they were, unharmed and freely enjoying their pond environment.

Hmmmm, maybe that's a way to protect data, too . . . data that protects itself by diving into a deep cryptographic pool when attacked; but that's another article.

\* \* \*

Jan Buitron took her first computer class in 1989, launching a long career in Information Technology. Starting in Technical Support, she methodically progressed from providing level 1 to providing level 5 support and beyond. She relentlessly pursued industry certifications, starting with two full Microsoft MCSE certifications, along with CompTIA's Network +. She attained the CISSP in 3.5 months. Most recently, she passed the ITIL v3 and CISM exams.

During seven years at IBM, she was introduced to information assurance as an Access Control administrator. Continuing her IA career, she participated in a Security Operations Center there, as well. Her experiences there prompted her to pursue a Master's Degree in Information Assurance (MSIA) from Norwich University, which she finished in 2009. She has since worked in IA for six different government agencies and the DoD.

Jan currently teaches for Regis University as adjunct professor in their Masters of Science Information Assurance Program, teaching classes such as Information Security in Enterprise Assurance and Computer Forensics.

She is an accomplished writer, with several articles in Network World. She wrote the soon to published a chapter covering security and privacy concerns in social networking for the 6th edition of the *Computer Security Handbook*, (Wiley). Her near-term plans include a PhD in Information Assurance.

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

Copyright © 2012 Jan Buitron & M. E. Kabay. All rights reserved.

Permission is hereby granted to *InfoSec Reviews* to post this article on the *InfoSec Perception* Web site in accordance with the terms of the Agreement in force between *InfoSec Reviews* and M. E. Kabay.

### **Pay Attention to Anomalies**

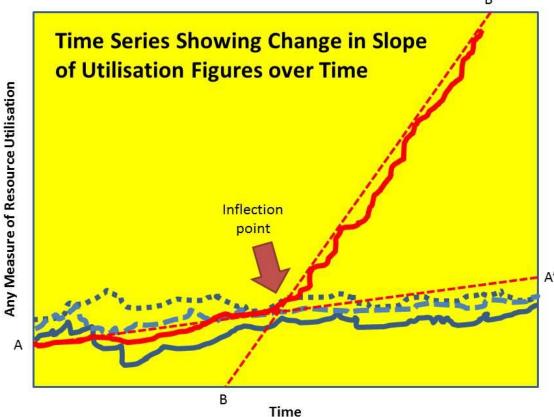
by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Today I increased my virtue coefficient by getting to the swimming pool up the road from where I live (well, 7 km from where I live in farming country) early in the morning. On my way out after a vigorous set of laps (I normally swim a "mile," which is an ancient measure of distance still used in backwaters such as the USA), I stopped at the desk to tell the attendant that I would like to switch my automatic payments from my credit card to a direct withdrawal from my bank account (VISA charges are rough on the profits of this small business in the wilds of Vermont and I'd like to do my part to help these folks out).

Jim the attendant looked me up on his computer and discovered that there had been no payments from my VISA account since last November: I owed six months of fees! Jim explained that there had been "some problems" with their admission and billing system after an upgrade in January, but that the problems were resolved now. He agreed that allowing members to default on their monthly dues was a serious threat to cash flow for this small organization. It seems that the software was *supposed* to issue a warning automatically to members about delinquent payments, but that part of the code never activated.

After paying the accumulated fees, I thought about how dangerous this glitch – this anomaly – was. This health club has a sign-in that uses a card swipe to bring up the members account on screen and shows a photo of the authorized user of the account – all in aid of user identification and authentication to prevent free riders who might share a single membership. In previous discussions with managers, I've urged them to monitor their records carefully for customer-relationship assurance; for example, if I were running the club, I'd bring up an exception report whenever any member's attendance figures dropped below a proportion of their normal activity. Someone who works out every day hasn't shown up for a week: are they ill? Are they on a trip or on vacation? An e-mail expressing concern would be a nice touch; perhaps the managers would respond to a sickness by offering the customer an extension on their account – you don't use the system for a month, you get the deadline extended by a month. Note that the critical issue in such a system is to define the anomaly in terms of what's normal for the specific member, not in terms of a general average. Thus if someone comes in once a week and misses a month, then perhaps that situation would prompt an enquiry.

I've taught students for decades that they should be paying attention to anomalies. Anomaly detection depends on adequate data gathering and statistical analysis – or even just graphical representation of the data. For example, the following diagram shows a typical anomaly: a change of slope.



In the diagram, the three blue lines at the bottom represent some normal changes in a resource; e.g., disk-space utilisation. The graphic reminds me of a good real-world illustration of the value of paying attention to anomalies.

Back in the mid-1980s (my goodness, almost 30 years ago!), I was the director of technical services for a computer time-sharing service bureau (we served 28 insurance companies and insurance brokerages) in Montréal, Québec, Canada. I remember a specific incident where I was using a graph with lines for disk space utilisation (when a huge HP7933< http://www.hpmuseum.net/images/7935-40.jpg > disk drive had 404MB – yes, megabytes, children, not terabytes) by different customers. In the case I am remembering, a customer's diskspace began growing at a furious rate (represented as the continuous red line in the diagram). The inflection point is where the slope in disk utilisation changed from the A-A' line to the B-B' line. Any time there's an inflection point, resource managers should become curious: what's happened to cause the inflection? Because I routinely monitored CPU utilisation and disk-space utilisation among other parameters, I spotted the change quickly and investigated. It turned out that programmer at the customer site had REMmed (commented out – from REMark) the instructions in the job control language (JCL) for a particular batch job so that temporary files wouldn't be deleted at the end of the job. After he ran his diagnostics, he forgot to remove the REMs. By the time I caught the anomaly, the client had about 20,000 temp files in their account. (By the way, that programmer should *not* have been using *production* code to run his tests.)

Even if a change in slope is not due to an error, noticing and investigating an inflection point is a good idea. For example, it could be that a new routine has been implemented on the date where

the slope has changed; in that case, system managers would want to notice the change in resource consumption and plan for orderly resource management (such as ordering new resources earlier or later than planned).

From an *information security* perspective, inflection points in resource utilisation can signal information system security officers (ISSOs) that something unusual has happened or that a norm is being redefined. For example, suppose that the graph above represented accumulated CPU utilisation or bandwidth utilisation for individuals or for specific workgroups in an organization. Wouldn't any ISSO want to know *why* there was a change? What if it were an unauthorized change? What if the system had been infected by botnet malware and the increased bandwidth was due to 10,000 spam e-mails being sent out per hour on a rogue Simple Mail Transport Protocol (SMTP) server<

http://www.blockdos.net/mind\_the\_egress\_when\_filtering\_for\_security.html >?

Another example: Joe the accountant has never logged into the network after working hours in the last six years of record-keeping; so what is happening when "he" starts logging in at 03:00 every day and is generating GB of data transfers? Wouldn't an ISSO want to check with Joe about what's up? And wouldn't it be important to discover that Joe has no idea what the ISSO is talking about? Aha! Unauthorized access: hacker at work.

Anomaly detection using resource utilisation data can't be invoked suddenly: unless there are accumulated data allowing analysts to establish norms, it may be difficult or impossible to distinguish random fluctuations from systematic changes. For those interested in automating their analytical tools, one would compute linear or nonlinear regression coefficients for moving subsets defined by some reasonable period (as a function of the intrinsic variability of the data) and note changes automatically for alerts to be signalled to the resource managers or ISSOs. Readers will want to consult any textbook of applied statistics for details.

So to sum up, keep track of resource utilisation and investigate anomalies!

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

## **Include Security in Brain Interfaces**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

My wife, Dr Deborah N. Black, MD, is an expert in neural feedback (NF) for improving the attention of patients with attention-deficit / hyperactivity disorder (ADHD). There's an interesting news story about the technique on National Public Radio (NPR)<
<a href="http://www.npr.org/templates/story/story.php?storyId=130896102">http://www.npr.org/templates/story/story.php?storyId=130896102</a> This approach to retraining disorderly brains monitors electroencephalographic (EEG) data as the subjects learn to focus better by playing video games or controlling the visibility of a favourite movie being played on a special DVD player or computer. There are many sites in the United Kingdom which advertise NF treatments; try search string "neural feedback adhd uk" in a search engine. For example, "Learning with neural feedback"</a> <a href="http://www.learningwithneurofeedback.co.uk/">http://www.learningwithneurofeedback.co.uk/</a> > has useful information about the technique.

Deborah's work has gotten me interested in following developments in the entire field of direct neural interfaces. Back in 1995, the film "Johnny Mnemonic" <a href="http://www.imdb.com/title/tt0113481/">http://www.imdb.com/title/tt0113481/</a> > imagined a world in which people had what appeared to be standard female phono jacks in their head; the character would plug a male phono jack <a href="http://upload.wikimedia.org/wikipedia/commons/thumb/9/93/Jack\_plug.png/300px-Jack\_plug.png">http://upload.wikimedia.org/wikipedia/commons/thumb/9/93/Jack\_plug.png/300px-Jack\_plug.png</a> > into his head to transfer data. The film mentioned that his brain could hold – gasp – 4GB of data! In recent years, a company called NeuroSky® <a href="http://www.neurosky.com/">http://www.neurosky.com/</a> > has been developing an increasingly wide range of applications of neural interfaces. They are particularly interested in increasing EEG-sensor availability to the research community <a href="http://www.neurosky.com/Academics/WhatWeDo.aspx">http://www.neurosky.com/Academics/WhatWeDo.aspx</a> >.

The future of such systems includes direct neural control of computer-equipped systems such as artificial limbs. In a recent article by Ian Sample entitled "Brain implant allows paralysed woman to control a robot with her thoughts," < <a href="http://www.guardian.co.uk/science/2012/may/16/brain-implant-paralysed-woman-robot-thoughts">http://www.guardian.co.uk/science/2012/may/16/brain-implant-paralysed-woman-robot-thoughts</a> > published in *The Guardian* on 16 May 2012, the author describes the ineffable joy of a woman identified only as "S3" when she managed to control a robotic arm mentally so that she was able to serve herself a cup of coffee for the first time since her stroke fifteen years ago. Another report<
a href="http://news.sciencemag.org/sciencenow/2012/05/paralyzed-patients-control-robot.html">http://news.sciencemag.org/sciencenow/2012/05/paralyzed-patients-control-robot.html</a> > from *Science Now* has additional details.

The studies described in the *Guardian* and *Science Now* articles use implanted electrodes in the brain; NeuroSky devices look more like earphones or headbands. I think we are only a few years away from seeing NeuroSky equipment and other lightweight, non-invasive systems for neural interfacing. There is great hope not only for disabled people who may regain control of their limbs or voices, but also for more general applications. For example, in 2008, there was news<a href="http://www.newscientist.com/article/dn13449-nervetapping-neckband-used-in-telepathic-chat.html">http://www.newscientist.com/article/dn13449-nervetapping-neckband-used-in-telepathic-chat.html</a> of a "neckband that translates thought into speech by picking up nerve signals" that was "used to demonstrate a 'voiceless' phone call for the first time."

If a neckband can translate neural input (thinking about what we want to say) into sound, it can eventually also be used for silent dictation and for controlling computers by programs similar to Dragon Dictation®.< <a href="http://www.nuance.com/talk/">http://www.nuance.com/talk/</a> > Eventually, it should be possible to achieve that staple of science fiction, the silent "phone" conversation: the sender's neural interface for interpreting imaged speech sends data to the recipient's neural interface for interpreting digital data to brain patterns corresponding to hearing a voice. Voilà! Artificial telepathy!

At this point, we turn to the issue of integrating security into new systems using thorough analysis of potential vulnerabilities and effective quality assurance methods. Anyone interested in seeing the consequences of trying to patch security into inadequately designed and implemented products need merely consult the extensive archives of the RISKS Forum: *Forum on risks to the public in computers and related systems*< <a href="http://catless.ncl.ac.uk/Risks/">http://catless.ncl.ac.uk/Risks/</a>>. I've aggregated<<a href="http://www.mekabay.com/overviews/risks/index.htm">http://catless.ncl.ac.uk/Risks/</a>>. I've aggregated<<a href="http://www.mekabay.com/overviews/risks/index.htm">http://www.mekabay.com/overviews/risks/index.htm</a>> the first 25 volumes of the RISKS Digest into PDF files for convenience of readers and also generated an Acrobat PDX global index for searching the PDF files. The *RISKS Digest* site has an excellent search engine ("swish-e") that finds keywords in less than a second.

For example, the latest issue of the *RISKS Digest* [26(84)]< <a href="http://catless.ncl.ac.uk/Risks/26.84.html">http://catless.ncl.ac.uk/Risks/26.84.html</a> > includes these and other reports on breaches of security principles resulting from inadequate analysis and testing:

- Availability: Delays in billing U\$1.6M in parking fines< http://catless.ncl.ac.uk/Risks/26.84.html#subj1 >
- Availability: Closing down a department of motor vehicles office< http://catless.ncl.ac.uk/Risks/26.84.html#subj2 >
- Integrity: University students received payments for tuition they never paid< http://catless.ncl.ac.uk/Risks/26.84.html#subj4.1 >
- Integrity: Flash crowd develops at a courthouse< http://catless.ncl.ac.uk/Risks/26.84.html#subj6.1 >
- Authenticity: Sliding fingers over number pads ("gestures") on mobile phones as an authentication method will fail if users have greasy fingers <
   <p>http://catless.ncl.ac.uk/Risks/26.84.html#subj14.1

My guess is that one of the most serious threats to neural interface systems is going to be man-inthe-middle attacks (MITMAs). Examples from *RISKS Digest* include the following (note that I used my own descriptions, not the actual article titles):

- Clipper chip was susceptible to MITMA
   <a href="http://catless.ncl.ac.uk/Risks/14.64.html#subj6.1">http://catless.ncl.ac.uk/Risks/14.64.html#subj6.1</a>
- HotJava 1.0 alpha 3 security issues allowed MITMAs
   <a href="http://catless.ncl.ac.uk/Risks/17.43.html#subj8.1">http://catless.ncl.ac.uk/Risks/17.43.html#subj8.1</a>
- A teenaged boy used a stolen pager to send faked medical instructions to hospital staff< http://catless.ncl.ac.uk/Risks/21.19.html#subj6.1 >
- Exploding mobile phone chips by remote control perfect situation for MITMAs< http://catless.ncl.ac.uk/Risks/21.87.html#subj1.1 >
- Home-banking online sessions were susceptible to MITMAs
   <a href="http://catless.ncl.ac.uk/Risks/22.37.html#subj6.1">http://catless.ncl.ac.uk/Risks/22.37.html#subj6.1</a>
- A proxy Web service was vulnerable to MITMAs
   <a href="http://catless.ncl.ac.uk/Risks/23.79.html#subj9.1">http://catless.ncl.ac.uk/Risks/23.79.html#subj9.1</a>
- Spyware program used fake certificates for potential MITMAs<

- http://catless.ncl.ac.uk/Risks/23.88.html#subj5.1 >
- A firewall used fake certificates for potential MITMAs< http://catless.ncl.ac.uk/Risks/25.50.html#subj10.1 >
- A Syrian MITMA against Facebook used fake certificates< http://catless.ncl.ac.uk/Risks/26.45.html#subj10.1 >
- A forged certificate claiming to be for Google.com supports MITMAs against GMAIL users and others< http://catless.ncl.ac.uk/Risks/26.56.html#subj12.1 >

A recent summary of mobile phone weaknesses<

http://www.nytimes.com/2012/01/26/technology/personaltech/protecting-a-cellphone-against-hackers.html > includes several examples of MITMAs on poorly secured phones.

So what can we envisage from neural interfaces controlling, say, computers, human prosthetic limbs, industrial robots and communications devices? How about these?

- The neighbour's kid intercepts your neural dictation signals and inserts rude words into your memo to the boss;
- A nasty pervert makes amputees dump their soda all over themselves or punches someone in the head using the victim's prosthetic arm;
- A murderer causes an innocent user of a neutrally controlled prosthetic leg to jump into heavy traffic;
- The industrial saboteurs from our favourite hacker haven intercept the neural-interface signals in a competitor's factory to make the industrial robot go berserk, leading to several deaths, many injuries and a murder conviction for the innocent controller;
- In the near future, when neural interfaces are the standard method for communicating silently through artificial telepathy, industrial spies intercept private communications and pranksters insert inappropriate content into conversations.

Failing to include security into the design of systems – any systems – leads to serious vulnerabilities – and in some cases, serious exploits. All communications between neural interfaces and actuators *must* be designed to resist MITMAs from the very start of design.

I will be contacting manufacturers of the current generation of neural interfaces for their comments on how they are integrating security into their systems and will summarize the results for readers in a later article – assuming any of the manufacturers are willing to discuss the issue.

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

### **Letter to a Chinese Spammer**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

In late May, I received the following e-mail message from someone in Guangdong, China using an English name:

Hi, we are manufacturer specialized in producing&designing OEM portable speakers for mp3/mp4/notebook/ipod and other mobile device.

It also has a Mp3 player function, but more than that. Play mp3 format music from TF card or U-disk. also there's FM radio function, you can share the news even in your trip or travel.

I found your company name&email address in E-market place.

I know you are selling brands in this field.but if you can put our products on your shelves,it will enlarge your products' range,and it will attract more new clients and give your old clients more services.

With its reasonable price and multi-function features, it will be a very good choice for gift or accessories for ipod/iphone,it's portable, with external rechargeable battery, you can take it anywhere anytime.

and I'm sure of that it will be fashion soon in your local market.

Your each enquiry will be appreciated very much and will be taken care very seriously. We believe the customers are our only lifeblood.

For more details of us,please visit our website.and we are gold supplier on Alibaba,please check the page.

Looking forward to hear from you soon.

Thanks&best regards

- English-name removed -

- company name removed -
- address details removed –

District, Shenzhen, Guangdong, PRC 518108

Tel:86-755-xxxxxxxx Fax:86-755-xxxxxxxxx Cell Phone:86-xxxxxxxxx

SKYPE: nnnnnnn

MSN:nnnnnn@hotmail.com

E-mail: nnnnnn@company-name,com

Irritated into actually responding to spam – not, in general, a wise decision – I sent "Mr Englishname" the following message:

Dear Mr "English-name",

I'm sorry to inform you that you have been the victim of criminal fraud.

The unsolicited commercial e-mail (UCE or "spam") that someone sent out on your company's behalf was NOT sent to the selected addresses that they claimed they would use.

For example, your spam mentions the recipient's "company" and falsely claims that it was found in "E-market place." I doubt that more than a tiny fraction of your recipients do in fact have anything to do with your business.

In addition, your supposed name, "English-name," is totally improbable for someone living in China – especially given the abysmal level of English used in the spam.

The people who tricked you must have (a) told you to lie; (b) immediately signaled to recipients that you cannot be trusted; and (c) demonstrated their own incompetence.

Did you know that much of the junk e-mail from received in the USA from China is entirely in Chinese ideograms? And that almost no one in the USA can read what has been sent? At least yours was in a semblance of English.

The people who wrote the garbage in your spam also inserted commas before the top-level domains in the e-mail addresses, rendering them useless. You will notice at the bottom of your junk that they listed your addresses with ",com" instead of ".com" in both cases.

Sending spam with such glaring evidence of stupidity naturally leads to a reasonable assumption that the senders are (a) naïve idiots and/or (b) criminals who are attempting to perpetrate fraud.

I strongly recommend that you demand the details of the e-mail distribution list that the criminals who defrauded your company used in their fraudulent scheme. They took your money under false pretenses. Given that you live in the People's Republic of China, where there is no effective rule of law, I recommend that you deal with the criminals personally. Stuffing several hundred paper copies of their fraudulent e-mail – e-mail that disgraces you and your company before the world – up their noses or other body orifices would be a highly appropriate punishment. You can also just illegally beat them severely, as that is a common technique used by your own police forces on anyone disliked by people in power. If they complain to the police, you can always bribe an officer or two to look the other way or to beat them some more.

It would be nice if you could spread the word to your colleagues in business in China so that fewer of you could make total fools of yourselves in the eyes of millions of unwilling recipients of your junk mail.

I sincerely wish you zero sales from your efforts and earnestly regret the embarrassment and humiliation before your entire family, community and nation.

Best wishes for better luck next time,

Mich

### [sigblock]

I actually got a response within a few seconds (usually a sign that we're dealing with an autoresponder); it said only "Thanks,Mich.[sic]" I wonder what will happen when the sender actually reads the message?

Out of interest, I went to my GMAIL account and counted how many of the spam messages used only Chinese ideograms. Results: 169 of 294 spam messages received between 10:58 (UTC-5) of Thursday, 24 May and 06:31 Saturday 19 May 2012 were entirely in ideograms – 57%.

Another message that I'd love to get to the new spammers all over the world is that < .EDU > or < .EDU. > addresses are used exclusively by educational institutions in the USA and around the world and therefore no one with such addresses could possibly be a potential distributor for their industrial products. See "EDUcating Spammers" for additional details and resources.

Readers should feel free to modify and store this text for future use. Maybe we can educate our Chinese colleagues to the reality of the criminals generating Chinese spam worldwide.

For what it's worth, I'll send a copy of this essay to the address<
<a href="mailto:chinaembpress">mailto:chinaembpress</a> us@mfa.gov.cn</a> listed on the Chinese Embassy's Website for the USA. I'm sure readers can find the equivalent for their own country – and feel free to send a copy of this article to your own local embassy's address! Who knows? Someone may actually get annoyed enough to arrange for the non-judicial punishment of *real* criminals in China instead of focusing only on the persecution of political enemies<
a href="http://www.nytimes.com/2012/05/25/world/asia/brother-of-chen-guangcheng-escapes-guarded-village.html">http://www.nytimes.com/2012/05/25/world/asia/brother-of-chen-guangcheng-escapes-guarded-village.html</a> of the ruling classes there.

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

### **Dum Spiro, Sperry**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Information Assurance& Statistics School of Business & Management Norwich University, Northfield VT

I've always had complaints about Microsoft Outlook's user interface. For example, I sent in a suggestion for Outlook 2007 years ago complaining about the user interface for e-mail rules: there was no way to select all the rules! Every time a user wanted to run rules, (s)he had to manually check all the rules one by one. There must have been enough identical complaints, because the 2010 version of Outlook includes SELECT ALL and UNSELECT ALL buttons in the RUN RULES pop-up box.

One problem that Outlook users face is duplicate entries. These can occur because a sender has something wrong with their e-mail configuration (e.g., one of my colleagues simply cannot stop his system from sending a copy of every e-mail as he is sending the original), or it may happen when a user imports messages from a different Outlook OST<<a href="http://office.microsoft.com/en-us/outlook-help/create-an-offline-folder-file-ost-HP005242261.aspx">http://office.microsoft.com/en-us/outlook-help/create-and-use-pst-data-files-in-different-versions-of-outlook-HP001231987.aspx?CTT=1</a>>file that may have been created at a different time or on a different computer.

Similar problems can occur with contacts and calendars; improper synchronization of one computer's Outlook data with, say, the data on a smart phone or tablet can result in duplicate entries. Microsoft's advice for eliminating duplicate messages or contacts<a href="http://office.microsoft.com/en-us/outlook-help/resolve-or-delete-duplicate-contacts-HP010355041.aspx?CTT=1">http://office.microsoft.com/en-us/outlook-help/resolve-or-delete-duplicate-contacts-HP010355041.aspx?CTT=1</a> is really simple: locate the duplicates, highlight them, and delete them by pressing DELETE. Unfortunately, if you have thousands of entries, the manual method is tedious and prone to error (such as not highlighting a duplicate or highlighting unique entries).

For some years, I used a free tool called Outlook Duplicate Items Remover (ODIR)<a href="http://www.vaita.com/ODIR.asp">http://www.vaita.com/ODIR.asp</a> which can locate duplicates in a single folder and move them to a subfolder. For 32-bit versions of Outlook, it worked well, although having to run it over and over for every folder was a nuisance when there were lots of folders (I keep hundreds). However, when I installed 64-bit Outlook 2010 on my 64-bit Windows 7 computer, the current version of ODIR failed and there's no 64-bit version available.

In looking for replacements, I came across the Outlook Add-Ins created and sold by Sperry Software<<a href="http://www.sperrysoftware.com/Outlook/default.asp">http://www.sperrysoftware.com/Outlook/default.asp</a>. The list of add-in utilities<<a href="http://www.sperrysoftware.com/Outlook/downloads.asp">http://www.sperrysoftware.com/Outlook/downloads.asp</a>> is impressive and includes functions many of which I have always wanted:

- Add Email Address: remembers to create a new contact record for any e-mail you use in a reply or a send.
- **Always BCC**: pops specified e-mail addresses into your CC or BCC field automatically. Never again fail include your boss on your distribution list if that's what (s)he wants.
- Appointments by Email: allow text e-mail messages to generate appointments for you.
- Attachment Forget-Me-Not: How many times have we forgotten to include an attachment in our e-mail message? I got so embarrassed about it that I created a text

The add-in lets us define words that trigger a reminder; e.g., "attached," "see document," "see file" and so on. If it sees a keyword but the sender doesn't need an attachment, it's a single click to ignore the reminder.

- Attachment Save: converts all attachments into files stored in a specified folder and puts a link to the file into the top or bottom of each message affected. When I applied this tool to my current PST file, the volume of the file went from 800MB to 400MB after compaction. Be careful, though: once the files have been moved to a folder, there is no easy way to change the location of the folder. However, the Undo Now function in the Utilities sub-menu for this tool will reintegrate the attachments so one can redo the move. There is also a function that changes the storage location and automatically modifies the links in all affected messages so that they are corrected. Why does this function matter to me? Because I define yearly archives (e.g., archive2011.pst) which are the renamed archive.pst file for that year.
- **Auto Print**: automatically print every e-mail on arrival (don't do that unless you absolutely have to: I strongly disapprove of putting messages on compressed plant fibres using pigments sprayed or fused on the fibre sheets unless absolutely necessary).
- **Compliance Copies**: use conditions to determine who should automatically be added to CC or BCC lists as a function of message content.
- **Contacts Sort Order**: ensure that all the contacts in Outlook follow a single format: < last, first > or < first, last >.
- **Distribution List Manager**: create a list from the TO or CC fields of a message with a single click. Also, "You can also easily see which DLs [distribution lists] a given contact belongs to."
- Duplicate Appointments Eliminator.
- Duplicate Contacts Eliminator.
- **Duplicate Email Eliminator**: works on one folder at a time to locate and remove duplicates.
- **Duplicate Email Eliminator Across Folders**: allows the user to compare the contents of a number of folders in a source list with a number of folders in a target list and eliminate the duplicates that are in the target folders. This single-pass function compares every message in the source folders with every message in the target folders. The process can lead to a combinatorial explosion and long run-times; for example, even with only 100 e-mail messages in two folders, we'd end up with (100\*100) = 10,000 comparisons. Mind you, if one makes a mistake and discovers the system wandering off into 100% CPU and disk I/O because of an error in the comparison lists, a simple click of the mouse interrupts the process so one can be more restrictive in defining the comparisons.
- Other duplicate remove add-ins cover journals, notes, posts to an Exchange folder and tasks. All the duplicate removers provide extensive options for defining what constitutes a duplicate; e.g., one can select any combination of characteristics such as Subject, Body, Attachments Count, Recipients Name, Sender Name, Importance, Received Time and Sent Time. One can also move the duplicates to a special folder or just delete them.
- **E-mail Reminders**: have appointments pop up in e-mail suitable for those who routinely access their e-mail on a mobile device.
- File Fetch: "With this add-in, you can retrieve a file from any of your Windows folders

- using just email."
- Follow Up Reminder: alerts when people fail to respond to e-mail messages.
- Global Search And Replace: ensures that changes to names are propagated throughout Outlook.
- **Help Desk Email** Templates: defines standard formats for submitting requests to the Help Desk for support.
- **Hide Fax Numbers**: prevents Outlook from tricking one into loading a fax number into a destination field.
- **Incoming Mail Organizer**: avoids crashing into the limit on the number of rules for sorting incoming e-mail into folders.
- **Insert Date/Time**: adds a button that inserts information such as current date, time and author into any element of Outlook.
- **Mobile Email Redirect**: sends important e-mail automatically to mobile device and allows the user to reply to the original sender(s).
- **Power Rules Manager**: manage Outlook e-mail-processing rules without being limited by the tiny window of the native program.
- **Reply To All Monitor**: removes user's own e-mail address from the REPLY ALL list and more important, asks the user if (s)he *really* wants to REPLY ALL!
- **Safeguard Send**: user can define keywords that will spark a prompt if a message seems to be violating confidentiality rules.
- Save as PDF: automatically converts any e-mail into a storable PDF file, including conversion of many types of attachments.
- Schedule Recurring Email: regular reminders at a click of a button.
- **Secure Email Forward**: control the content of e-mail forwarded outside the organization.
- **Send Individually**: converts a distribution list into individual e-mail messages.
- **Sent Items Organizer**: defines where send e-mail should be stored by keyword or using a prompt.
- **Think Green**: the opposite of Auto Print asks the user if (s)he *really* needs to print an item.
- **Time Date Signature**: add the date and time at the moment of pressing SEND rather than relying on system-generated time-stamps that may mislead the recipient by using a later time in the e-mail headers.
- Vcard Converter: converts all contacts to individual vCards.
- Watch Folders: sends an alert "whenever an item in a public folder or mailbox is changed" in an Outlook shared folder.

Whew! I've already installed and bought licenses for Attachment Forget-Me-Not, Attachment Save, Contacts Sort Order and Eliminate Duplicates Across Folders. I may very well buy some more!

By the way, the title of today's column is a joke based on the Latin motto "Dum spiro, spero," which means "While I breathe, I hope."

[Note: I have no financial association with this company and have not received free software or payment for this review. I did have a very nice chat with the founder, Mike Sperry<<a href="http://www.linkedin.com/pub/mike-sperry/2/5a8/90">http://www.linkedin.com/pub/mike-sperry/2/5a8/90</a>> who happened to answer the tech support phone when I called with a question.]

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

# **Identifying Fraudulent Work-at-Home Scams**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Recently I got an e-mail message from a naïve young person who was excited about the riches available through part-time work at home posting links to products on the Web. I hope that the approach to spotting fraud will be useful to other potential victims; please feel free to circulate it among your colleagues at work as part of any security-awareness program.

```
From: ---
      Date: Wednesday, May 23, 2012 15:11
      To: - a bunch of people who don't necessarily know each other -
      Subject: I am my own boss try it out for yourself
      How to Get Rich using your PC
      http://doctoraluisazitzer.com/disclog24.php?jID=7xovx
* * *
      Hi ---,
      This is almost certainly fraudulent.
      1) Although the link is for < doctoraluisazitzer.com > in fact the link
      connects to a different Website entirely < corporateincomefromhome.net
      >. Having an immediate switch of link is inherently deceptive. In
      addition, the ownership records about doctoraluisazitzer.com available
      through BETTERWHOIS.COM< http://betterwhois.com/ > show the following
      data (spelling mistakes are in the original):
      [Querying whois.dattatec.com]
      [whois.dattatec.com]
      Datttatec.com - Registration Service Provided By: Dattatec.com
      Contact: +54 341 599000
      Email: dominios@dattatec.com
      Website: http://www.dattatec.com
      Domain name: doctoraluisazitzer.com
      Creation Date: 2011-06-18
      Expiration Date: 2012-06-23
      Status (es):
         OK
      Domain Name servers(es):
        ns1.traxhost.com
        ns4.hostmar.com
        ns2.dattaelite.com
         ns3.hostmar.com
         ns22.dattatec.com
         ns21.dattatec.com
      Registrant conatct:
```

Name: Luisa Zitzer Company: Luisa Zitzer

Email: aletitor2@hotmail.com

Address: a

AR - a ( zip: - ) Phone : 54 - 8327920

#### Admin conatct:

Name: Luisa Zitzer Company: Luisa Zitzer

Email: aletitor2@hotmail.com

Address: a

AR - a ( zip: - )

Phone : 54 - 8327920

#### Billing conatct:

Name: Luisa Zitzer Company: Luisa Zitzer

Email: aletitor2@hotmail.com

Address: a

AR - a ( zip: - )

Phone : 54 - 8327920

#### Tech conatct:

Name: Luisa Zitzer Company: Luisa Zitzer

Email: aletitor2@hotmail.com

Address: a

AR - a ( zip: - )
Phone : 54 - 8327920

The country code 54 corresponds to Argentina!

2) Here is the registration information about the domain < corporateincomefromhome.net >: it's RUSSIAN. Russia is one of the main centers for worldwide credit-card fraud. Type "Russian federation credit-card fraud" into the GOOGLE search field (without quotation marks) for more news about the issue than you want to read.

[Querying whois.ukrnames.com]

[whois.ukrnames.com]

Service Provided By: Center of Ukrainian Internet Names

Website: http://www.ukrnames.com

Contact: +380.577626123

Domain Name: CORPORATEINCOMEFROMHOME.NET

Creation Date: 23-May-2012 Modification Date: 23-May-2012 Expiration Date: 23-May-2013

Domain servers in listed order:

ns1.okeraafrer.ru
ns2.okeraafrer.ru
ns3.okeraafrer.ru

#### Registrant:

Olga Golubeva chapoohnet@gmail.com ul. Pushkina 98 56

Barnaul, 656000 RUSSIAN FEDERATION Billing Contact:
Olga Golubeva chapoohnet@gmail.com
ul. Pushkina 98 56
Barnaul, 656000
RUSSIAN FEDERATION
+7.4955467812

Administrative Contact:
Olga Golubeva chapoohnet@gmail.com
ul. Pushkina 98 56
Barnaul, 656000
RUSSIAN FEDERATION
+7.4955467812

Technical Contact:
Olga Golubeva chapoohnet@gmail.com
ul. Pushkina 98 56
Barnaul, 656000
RUSSIAN FEDERATION

- 3) The Web page pretends to be a news story from "NEWS DAILY 7." It is not: it's completely fake and has been created by the criminals. It inherently has ZERO credibility. In addition, the stories describe salaries up to \$8,000/month, not the \$10,397 in the headline.
- 4) Scamadvisor.com reports a ZERO trust rating for the site: see <
   http://www.scamadviser.com/is-corporateincomefromhome.net-a-fakesite.html >
- 5) The use of a .net top-level domain (TLD) for a commercial page is a warning sign; .net is supposed to be restricted to "organizations involved in networking technologies". See < <a href="http://en.wikipedia.org/wiki/.net">http://en.wikipedia.org/wiki/.net</a> >. Using that TLD gives the criminals a false veneer of respectability. To use .net for a profit-making organization instantly sets alarm bells ringing.
- 6) Work-at-home scams are well known to be used by criminals. See Alison Doyle's "Work at Home Scams." <a href="http://jobsearch.about.com/cs/workathomehelp/a/homescam.htm">http://jobsearch.about.com/cs/workathomehelp/a/homescam.htm</a> >
- 7) The links to "Home Business Idea" claim to be linking to < http://corporateincomefromhome.net/business-news-all/go.php > but they actually go to < http://thesecurepagee.com/e/HICM4/?misc1=855-230-3394&caid=29002&misc3=200674&caCode=HCML97G&nopop=0&stid=363&cid2=7474 > which is labeled "Home Income Ca\$h Machine" and claims impressively to be advertised on MSNBC, FOX NEWS, ABC, USA TODAY and CNN. However, you can instantly find several complaints about fraud involving this group: type "home income ca\$h machine" (without the quotation marks) into GOOGLE to locate complaints from people who were cheated out of \$100-\$300.
- 7a) < <a href="http://reviewopedia.com/workathome/home-income-cash-machine-reviews-legit-or-scam/">http://reviewopedia.com/workathome/home-income-cash-machine-reviews-legit-or-scam/</a> > reports,

"However, Home Income Cash Machine significantly misrepresents this opportunity when they say you are "paid to post links." You are not paid to post links. You are paid when the link you post results in a sale for that company. Unfortunately, that is very different. Instead of being paid every 4 minutes for the link you post, you would be paid

every time a sale goes through, which unfortunately is not likely to be every  $4\ \mathrm{minutes.}''$ 

Also "What You Should Know About Home Income Cash Machine

Home Income Cash Machine is selling a certification program for link posting. However, you do not need to be certified in link posting to work in affiliate marketing. It is an independent business opportunity, available to anyone.

Also, while their sales page says their program costs \$49.95, the reality is that it actually costs \$99.95. You have the option to get a \$50.00 rebate if, when you receive the welcome email, you agree to take a survey. If you do not take the survey, you will not get your rebate.

Finally, they have a very specific and difficult refund policy. While they claim to have a 60 Day Money Back Guarantee, the truth is that to get your refund, you must following their training and use their program for 60 days, exactly.

If, at the end of 60 days, you can prove you used their program the entire time and failed to make back the money you invested in the program, then you have 7 days to request a refund. Additionally, the Home Income Cash Machine website states that were you to request your refund before you have tried the program for 60 days, you would forfeit your ability to qualify for a refund."

7b) < http://www.scambook.com/report/view/112444/Home-Income-Cash-Machine-False-Advertising-for-134.00-on-05-10-2012 >

"Home Income Cash Machine - False Advertising for \$134.00 on 05/10/2012

I had thought it was a legitimate website to start making money but boy was I wrong. They claim that it is only \$97 to get started, so foolishly, I paid. I then was prompted to pay for other packages. As I continued, I never received my so-called "kit" so I tried contacting the company. Well, their email as well as phone number were both FAKE. I am now trying to deal with my credit card company to settle this dispute to get my money back and out of the hands of those crooks!

Submitted by J on May 10th, 2012"

7c) < <a href="http://www.scambook.com/report/view/112493/Home-Income-Cash-Machine-False-Advertising-for-97.00-on-05-08-2012">http://www.scambook.com/report/view/112493/Home-Income-Cash-Machine-False-Advertising-for-97.00-on-05-08-2012</a> >

"Home Income Cash Machine - False Advertising for \$97.00 on 05/08/2012

I too got scammed by what I thought to be a legitimate way to work at home. When I opened the site I was lucky and had good software to catch the viruses before they ruined my computer. It's bad enough to scam people but to ruin a persons computer worth hundreds of dollars is sick!! I also got calls from people saying they were calling to help, but in reality they were trying to gather information to steal your identity. Beware of this scam.

Submitted by Anonymous on May 10th, 2012"

7d) < http://workathomereviewers.com/home-income-cash-machine-review >

This Web site has excuses for the fraud attacks and includes "Many people have problems with work at home offers saying that they are

misrepresented and you can't really make the money they are talking about. The fact is there are many people who will make the amount of money advertised it just depends on how much effort they put into it and how well they do the job. Just like anything else in life, the return you see from this program directly reflects how much time you spend working on it and really learning it correctly." However, the BETTERWHOIS.COM service shows that the owners of "WorkatHome Reviewers" have chosen to conceal their identities — not a sound basis for inspiring trust. My guess? The people running home income ca\$h machine own the "review" site as well:

```
Registration Service Provided By: Namecheap.com
Contact: support@namecheap.com
Visit: http://namecheap.com
Domain name: workathomereviewers.com
Registrant Contact:
  WhoisGuard
  WhoisGuard Protected ()
  11400 W. Olympic Blvd. Suite 200
  Los Angeles, CA 90064
Administrative Contact:
  WhoisGuard
  WhoisGuard Protected
(b329987c37ed4db3bbbd4719df605de4.protect@whoisguard.com)
   +1.6613102107
   Fax: +1.6613102107
   11400 W. Olympic Blvd. Suite 200
  Los Angeles, CA 90064
  US
Technical Contact:
  WhoisGuard
  WhoisGuard Protected
(b329987c37ed4db3bbbd4719df605de4.protect@whoisquard.com)
  +1.6613102107
  Fax: +1.6613102107
   11400 W. Olympic Blvd. Suite 200
  Los Angeles, CA 90064
  US
Status: Locked
Name Servers:
  ns1.cpanelgold.com
  ns2.cpanelgold.com
Creation date: 08 Nov 2011 01:58:00
Expiration date: 07 Nov 2013 17:58:00
```

\* \* \*

In future, remember the simple rule: if it sounds too good to be true, it is. And don't send copies of exciting money-making offers you find on the Web to your friends until you check out the pages' legitimacy. Finally, since I'm in advising mode, never put a distribution list in the CC field unless the people have to

communicate with teach other: use the BCC field. See <
http://www.mekabay.com/infosecmgmt/emailsec.pdf > for guidelines on e-mail usage.

Best wishes,

Mich

=>o ASCII ribbon campaign against HTML e-mail o<=

Something I thought of later: there's a different kind of work-at-home scam involving reshipping products. For details, see SNOPES.COM report "Reshipper scam" <a href="http://www.snopes.com/crime/fraud/reshipper.asp">http://www.snopes.com/crime/fraud/reshipper.asp</a> > and the United States Postal Inspection Service short films "Work@Home Scams: They Just Don't Pay" <a href="http://www.mekabay.com/cyberwatch/uspis\_wahs.zip">http://www.mekabay.com/cyberwatch/uspis\_wahs.zip</a> > and "Dialing for Dollars" <a href="http://www.mekabay.com/cyberwatch/uspis\_dfd.zip">http://www.mekabay.com/cyberwatch/uspis\_dfd.zip</a> >

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

### Glasshouse: Stross – Never Dross

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

In 2008 I wrote a glowing commentary<

http://www.mekabay.com/nwss/623 halting state a good read for security geeks.pdf > about Charles Stross's < http://www.antipope.org/charlie/fiction/faq.html > 2007 novel *Halting State* < http://www.amazon.com/Halting-State-Ace-Science-Fiction/dp/0441016073/ >.

I've just finished reading an earlier work by Stross, *Glasshouse*, originally published in hardback by Ace and also available in paperback< <a href="http://www.amazon.com/Glasshouse-Charles-Stross/dp/0441015085/">http://www.amazon.com/Glasshouse-Charles-Stross/dp/0441015085/</a>, Kindle< <a href="http://www.amazon.com/Glasshouse-ebook/dp/B001161L60/">http://www.amazon.com/Glasshouse-ebook/dp/B001161L60/</a> > and audiobook< <a href="http://www.amazon.com/Glasshouse/dp/B004YLYJ4O/">http://www.amazon.com/Glasshouse/dp/B004YLYJ4O/</a> >. I think readers with an interest in computing, information assurance, and nanotechnology will find it immense fun.

I'd hate to spoil the book for readers by giving too much detail about the plot; I'll just quote a short summary posted on Amazon:

When Robin wakes up in a clinic with most of his memories missing, it doesn't take him long to discover that someone is trying to kill him. It's the 27th century, when interstellar travel is by teleport gate and conflicts are fought by network worms that censor refugees' personalities and target historians. The civil war is over and Robin has been demobilized, but someone wants him out of the picture because of something his earlier self knew. On the run from a ruthless pursuer, he volunteers to participate in a unique experimental polity, the Glasshouse, constructed to simulate a pre-accelerated culture. Participants are assigned anonymized identities: it looks like the ideal hiding place for a posthuman on the run. But in this escape-proof environment, Robin will undergo an even more radical change, placing him at the mercy of the experimenters--and the mercy of his own unbalanced psyche.--From publisher description.

Stross appeals to our inner geek: he packs his book with interesting titbits [US readers, don't get excited: that's what we write as *tidbits*] that are fun for the technically literate. For example, there's a note before the start of the novel proper that gives the reader translations from the 27th century's time measurement units; here are some of them:

- 1 second: "... The time taken for light to travel 299,792,458 meters in vacuum;
- 1 kilosecond: 16 minutes;
- 1 megasecond: 11 days, 6 hours;
- 1 gigasecond: 31 Earth years.

Here are some of the neat technologies introduced in the novel in the first few pages (the names I've given to the techniques are not necessarily those used by the author):

• Modifying bodies to suit functional needs or personal preferences: "A dark-skinned

human with four arms walks toward me across the floor of the club, clad only in a belt strung with human skulls. Her hair forms a smoky wreath around her open and curious face. She's interested in me."

- Identity restructuring: "It's tough, not being able to tell the difference between your own thoughts and a postsurgical identity prosthesis."
- Backing up one's entire memory so as to be able to regenerate a fresh instantiation of oneself if the current body dies unexpectedly: "I emigrated to Zemlya right after my previous memory dump."
- Metempsychosis: "I haven't been human for long.... I just moved here from Zemlya.... For my surgery.... I was an ice ghoul."
- Information transfers at transluminal velocity: "Traffic between polities, like traffic within a polity, passes over T-gates, point-to-point wormholes linking distant locations."
- Matter disassembly and reassembly [US spelling in original]: "My job, as part of the frontier guard, was to make sure that inbound travelers went straight into an A-gate an assembler array that disassembled, uploaded, and analyzed them for threats, before routing them as serial data to another A-gate on the inside of the DMZ for reassembly."
- Nanoscale engineering: "The ability of nano assembler arrays to deconstruct and replicate artifacts and organisms from raw atomic feedstock made them virtually indispensable not merely for manufacturing and medical purposes, but for virtual transport (it's easier to simultaneously cram a hundred upload templates through a T-gate than a hundred physical bodies) and molecular firewalling."
- Malware affecting gates self-reproducing programs have affected A-gates by censoring memories and ideas in the reconstructed entities: "Even when war exposed them to subversion by the worms of censorship, nobody wanted to do without the A-gates to grow old and decrepit, or succumb to injury, seemed worse than the risk of memory corruption."
- Sophisticated artificial intelligence: "Today's therapist isn't remotely humanoid, not even bushujo or elven; Piccolo-47 is a mesomorphic drone, roughly pear-shaped, with a variety of bizarre-looking extensible robot limbs some of them not physically connected to Piccolo's body and nothing that resembles a face."
- Synthetic pheromones to affect people's moods: "Piccolo-47's voice oozes with reassurance. I'm pretty sure it's a emitting a haze of feel-good pheromones..."

Without revealing any more of the book's details, it's a wonderful read for technophiles. Stross routinely assumes knowledge of security and networking concepts in the way that 19<sup>th</sup> century authors incorporated hydraulics and pneumatics, early 20<sup>th</sup> century writers included airplanes and radio, and late 20th century science fiction novelists took computers and data networks for granted.

Stross has an extensive list of novels; they are described on a frequently-asked questions page< <a href="http://www.antipope.org/charlie/blog-static/fiction/faq.html">http://www.antipope.org/charlie/blog-static/fiction/faq.html</a> > in his blog. I heartily recommend his work.

Enjoy!

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information

Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a>

\* \* \*

## **Data Integrity and Personal Integrity**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

A friend and colleague (let's call him Salil) recently got hired by a major international manufacturer of high-technology products (let's pretend they are, say, integrated gateway security/intrusion detection/intrusion prevention devices). The company has major government and private organizations as customers all over the world and has a staff of about 60.

Salil has 30 years of experience in high-technology sales and marketing, including extensive experience prospecting for and closing government contracts. He's an expert at writing responses to requests for proposals (RFPs) and is brilliant, creative, imaginative, and personable. He's one of the nicest people I've ever worked with; as a former rock-climber (long ago), I say that I would let him hold my rope – that is, I'd trust him with my life.

The interview process took a couple of weeks, with meetings between Salil and the human resources manager, the director of sales, and finally the president (owner, founder) of the company. Salil really hit it off with everyone he spoke with and several of his colleagues (including me) gave him excellent references by phone.

Salil started work on a Monday. That morning, he met with the sales manager and several members of the sales team. Within an hour, he was looking through the sales database that recorded all the contacts made by the company over the last 15 years. In passing, he was shown an Excel spreadsheet that was an extract from the database – except that it couldn't actually be an extract any more: it contained entries that were not in the database as well as some entries that were different from those in the database for the same customers.

#### What had happened?

The staff had committed the classic error of naïve computer users: they modified what should have been a read-only copy of the data. They thus ended up with the classic result of such parallel modifications: inconsistency.

Salil and one of the sales staff slaved over the database for about 10 hours that Monday and the next day looking for the correct data and updating the database. They were pleased with the results and Salil then turned to looking at the rest of the information infrastructure for the sales group. Conditions were not good.

- The Web site was essentially a copy of one of the company's old sales brochures. Linkages were minimal and there was no easy way to update any given component without redoing the entire page.
- Every component on the site was completely static: not one dynamic image, not one video, not even a search field.
- Several links were 404s (broken).
- There were a few e-mail addresses on the "Contact Us" page but two of them were out of date and would result in an e-mail bounce if anyone used them. There was no online

message form with a CAPTCHA< <a href="http://www.captcha.net/">http://www.captcha.net/</a> > (Completely Automated Public Turing test to tell Computers and Humans Apart) to defeat spammers, either.

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

## Facilit{ating,ies} Security

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Recently I was at a local shop and noticed a potential problem. See if you can identify it from the picture below showing part of the air conditioner on the outside of the building:



The problem is the unlocked cover to the left of the centre in the photo; it covers the circuit breakers. I asked the shop clerk whether the air conditioning was important for the shop; indeed it is, she said, as it maintains appropriate temperatures for non-refrigerated foods in the shop. The shop has already suffered vandalism; hoodlums broke one of its windows and its glass door during a night-time robbery. Leaving open access to switches that turn off the power for the unit is an invitation for further trouble.

Starting in the 1980s, I specialized in facilities security and in particular, hospital security. The worst case I ever encountered involving an electrical panel was in a Montreal hospital. I called the head of the intensive care unit (ICU) out into the public hallway from her office and pointed at a grey metal panel on the wall. "Do you know what that is?" I asked. She looked at me as if I was crazy. "Yes," she said, "it's an electrical panel," and looked at me as if to add, "Duhhh." I opened the panel and she turned pale: the breaker switches were clearly labelled with the names of critical equipment in the ICU such as heart monitors and iron lungs. If a passer-by had switched any of those breakers off, people could have died. With open access to the public in the hospital, the risk of tragedy was increased by the failure to lock that panel.

Typing < physical security overlooked > into the Google search engine (without the < >) brings up several articles making the point that physical security is often overlooked in today's technology-intensive information assurance. For example,

- Barker, D. (2008). "Is physical security overlooked in lieu of network security?" Tales of a Network Security Engineer – David Barker's blog (5 Sep 2008). < <a href="http://areyouvulnerable.com/?p=12">http://areyouvulnerable.com/?p=12</a>>
- Higgins, K. J. (2006). "The 10 Most Overlooked Aspects of Security." Security Dark Reading (29 Nov 2006). <a href="http://www.darkreading.com/security/news/208808177">http://www.darkreading.com/security/news/208808177</a> >
- Krupa, A. S. (2003). "The Oversight of Physical Security and Contingency
- Planning." SANS Institute Information Security Reading Room. <
   <a href="http://www.sans.org/reading\_room/whitepapers/recovery/oversight-physical-security-contingency-planning\_557">http://www.sans.org/reading\_room/whitepapers/recovery/oversight-physical-security-contingency-planning\_557</a>>
- Posey, B. M. (2003). "Don't overlook physical security on your network." TechRepublic (3 Apr 2003). < <a href="http://www.techrepublic.com/article/dont-overlook-physical-security-on-your-network/5032930">http://www.techrepublic.com/article/dont-overlook-physical-security-on-your-network/5032930</a>>
- Seiden, M. & B. Weis (2004). "Physical Security the Good, the Bad, and the Ugly." Physical security workshop at 21<sup>st</sup> Chaos Communication Congress (CCC) by Chaos Computer Club. Berlin, Germany, 28 Dec 2004). Posted to YouTube (2 Jan 2012). < <a href="http://www.youtube.com/watch?v=-4IIAKLCN-w">http://www.youtube.com/watch?v=-4IIAKLCN-w</a> > Meaningful content begins at 03:20 after a load of blather.

A document I prepared for students and clients is available for anyone to use in security assessments, education or training: "Facilities Security Audit Checklist" <a href="http://www.mekabay.com/infosecmgmt/index.htm">http://www.mekabay.com/infosecmgmt/index.htm</a> >. Major sections include

- 1. Fire hazards
- 2. Water
- 3. Air conditioning
- 4. Electricity
- 5. Preparing for civil, man-made, and natural disasters
- 6. Alternate location
- 7. Access control
- 8. Housekeeping
- 9. Miscellaneous

Checking physical security is relatively easy, but it requires a shift of focus. As in any security assessment, the trick is to notice details that affect assurance; the analyst should be thinking of possible problems and vulnerabilities to malicious insiders and outsiders. The best way to learn is to use a checklist in a walkabout: actually going through a facility looking at everything with a sceptical eye. The checklist may stimulate readers' imagination: just imagine what the Bad Guys could do with that unlocked electrical panel. . . .

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

## A Rich Vein: Huebner's New Blog

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Recently I found out that my friend and colleague Prof Richard Huebner < <a href="http://www.linkedin.com/in/richhuebner">http://www.linkedin.com/in/richhuebner</a> > began a new blog < <a href="http://www.db-geek.com/">http://www.db-geek.com/</a> > in May 2012. I interviewed Rich for our InfoSec Perception column.

1) Rich, tell us about your career.

I began using computers at age 10, when I learned how to program in BASIC on a Vic-20 and Apple IIc/IIe. I began my career in the early 1990s while working for an Internet service provider, called TIAC (The Internet Access Company). I began working as a customer service representative – it was dial-up at the time, with a maximum speed of about 56kbaud. Since then, I've had the pleasure of working for some pretty big places, including AstraZeneca, National Grid, John Hancock, in senior level positions in customer support, project management, and database administration. I've also had the opportunity to work with Harte-Hanks Data Technologies, Northern Power Systems, and the Department of Homeland Security (DHS). One of my recent accomplishments is the development and implementation of two new systems to optimize the work done by a team of 30 analysts working to resolve data-quality problems. Within days of implementing these systems, the productivity of all of the analysts skyrocketed. I was also able to eliminate much of the paper work being done by those analysts.

After a two-year hiatus from teaching, I came back to Norwich University<
<a href="http://www.norwich.edu">http://www.norwich.edu</a> in the fall of 2011. I am now entering my ninth non-consecutive year of teaching full time in higher education, and have also taught as an adjunct for Kaplan University<
<a href="https://www.norwich.edu">URL</a> >, Champlain College<
<a href="https://www.norwich.edu">URL</a> >, Eastern Nazarene College<
<a href="https://www.norwich.edu">URL</a> >, and Mount Vernon Nazarene University<
<a href="https://www.norwich.edu">URL</a> >, Eastern Nazarene College<
<a href="https://www.norwich.edu">URL</a> >, and Mount Vernon Nazarene University<
<a href="https://www.norwich.edu">URL</a> >.

The faculty and students at Norwich are fantastic people. On any given day, I get to work with the smartest people I have ever had the pleasure of working with – and that's what keeps me energized. Two of my friends, Drs M. E. Kabay and Peter R. Stephenson are people whom I deeply admire and look up to in terms of their kindness, professionalism, and mentoring and always get me energized when I'm around them! [MK adds: OK, Rich, we'll transfer the payment after this article is published!] I hope to stay with Norwich University for a very long time – it's one of the best places I've ever worked.

2) I see an increasing focus on security in your writing – when and why did you become interested in information security?

The DHS position I mentioned before was as a contractor working with the Fugitive Operations Support Centre (FOSC), in Williston, VT securing US borders from illegal and criminal aliens. It was absolutely fascinating and pushed my interest in security to the next level.

When I began my PhD studies at Nova Southeastern University< <u>URL</u> >, the school was offering several security courses and if I took them, I would get a graduate certificate in information

assurance/security. I've been interested in security since I began my computing career in the early 90s, I remember learning about Kevin Mitnick, Cap'n Crunch, and people like Steve "Woz" Wozniack. There were hackers in the true sense of what hacking used to mean. Today hacking means something bad, usually. Those guys were geniuses when it came to tinkering, so at the time I looked up to them even though I later realized that they sometimes broke laws. As I grew in my career, I realized that attacks could come from the person sitting in the next cube – not that I became paranoid, but I realized that attacks could come from anywhere. The attacks of 9/11 also made me (and many other people) realize that security is extremely important on many, many levels – from a national level down to a single firewall or intrusion detection system sitting in a network closet in the back office.

I decided to focus most of my energy reading and writing on the insider-threat phenomenon. I was very highly motivated by a former professor, who still believes that an attack is an attack is an attack. I disagree. Different types of attacks need different types of responses, and the insider threat is certainly complex enough to warrant different types of mitigation strategies.

3) Tell us about your plans for your new blog. Who's it for? What do you want readers to gain from your writing?

My overall goal is to make databases and database design more accessible to those who want to learn more, but don't necessarily want to learn every possible detail.

Part of the reason why I began this blog is simply to get my thoughts out and expand my reach so that others may be interested by some of the work that I do. My interests are pretty varied, from insider-threat research, to hands-on database design and development. The blog is being marketed to people who are not necessarily experts, but who want to learn more about various topics in database theory and information assurance. I make my posts straightforward and short and explain complex topics in a way that I hope will be accessible to anyone who wants to learn.

I'm also using the blog as a way to monetize some of the software and short e-books that I've developed along the way. For example, I have an 80-page booklet that I'm working on that discusses how to use MySQL and is a highly visual tutorial. The e-book assumes that you do not have a background in databases, either. I'd like to see the booklet being used more widely and will be making it available online soon.

In late May 2012, I met a wonderful person by the name of Jaime Utt<
http://www.jamieutt.com/index/Home.html >, who is a speaker on diversity and inclusion<
http://www.cultureofcivility.com >. I saw him speak at the Vermont Hugh O'Brian Youth
Leadership (HOBY)< http://www.hobyvt.org/ > seminar, and we got to talking. He mentioned
that he and his production company were having issues with their Websites, so I offered to help.
Jaime introduced me to Eric Thompson< http://www.linkedin.com/pub/ericthompson/44/77b/477 >, CEO of Global Ascension Productions<
http://www.globalascensionproductions.com/ >. Eric is an executive coach who has agreed to
help me better brand myself, and will be providing his coaching to me in exchange for
essentially being his chief information security officer (CISO). It is a bartering agreement, so no
money is exchanged. I don't really want his money, either – what I really needed was his
brilliance. He gets my expertise in return for providing me with his. Eric has been instrumental in
helping me establish my blog, what I should be doing, and in marketing my own brand, and
helping me unleash my own talents.

4) What are some of the key issues you plan to address in upcoming months?

I'm working on two series this summer: the first is on insider threats, and the second is on SQL injection issues. The insider threat problem is still heavily researched and there are plenty of proposed models and strategies for dealing with them, but I don't see evidence of their actually being used in practice. Essentially, I'm attempting to close the research/practice gap in coping with insider threats. In a forthcoming post, I'll be discussing two of the behavioural models we can use to help us begin identifying and mitigating insider threat risks.

SQL injection is such a hot topic right now that I had to chime in because I see some misinformation out there on the topic. Many folks most likely have a cursory understanding of it, so it's my hope that I can help solidify people's understanding of it and clear up any misconceptions.

5) What's your approach to handling comments from readers – and spam from creeps – on your blog? What are your thoughts about moderated lists and "anonymous coward" postings?

I have several Wordpress< <a href="http://wordpress.org/">http://wordpress.org/</a> > plugins that I use to keep tabs on comments. For example, one plugin will blacklist a post if it contains one of about 200 swear words or defamatory language. There are unfortunately a lot more words I could use to weed out profanity, but this is a start! Another plugin is specifically designed to exclude spam. Many of the pages on my site don't allow comments or feedback; however, most of the posts will allow moderated commentary. There may be some unmoderated discussions as well.

I'm also working on a member-only section to provide access to more depth and one-page executive summaries of various topics.

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

Copyright © 2012 Richard Huebner & M. E. Kabay. All rights reserved.

# Transforming Apathy into Action: Applying Recent Research on Prosociality to the Culture of Security

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

In 1993, I caused a stir in the world of information assurance by reviewing the applicability of well-established insights from social psychology to information assurance.<
http://www.mekabay.com/infosecmgmt/Soc\_Psych\_INFOSEC.pdf > Apparently no one up to that time had bothered to make explicit reference to social psychology for insights into the management of information security. The work was revised for inclusion in the fourth and then in the fifth edition of the Computer Security Handbook.< http://http://www.amazon.com/Computer-Security-Handbook-Volume-Set/dp/0471716529 > As my colleagues and I prepare for the publication of the sixth edition, due in October 2013, all of us are updating our chapters. Here's a paper that I am including in the social-psychology-and-infosec chapter in the next edition. As always, I am grateful to my dear father-in-law, Dr Percy Black, Emeritus Professor of Social Psychology, for his kindness in bringing this paper to my attention.

\* \* \*

Emma F. Thomas< <a href="http://www.psychology.murdoch.edu.au/staff/thomas.html">http://www.psychology.murdoch.edu.au/staff/mcgarty.html</a> > and Kenneth I. Mavor<
<a href="http://psychology.anu.edu.au/\_people/people\_details.asp?recId=126">http://psychology.anu.edu.au/\_people/people\_details.asp?recId=126</a> > published an article in the November 2009 issue of *Personality and Social Psychology Review* 13(4):310-333 entitled "Transforming 'Apathy into Movement': The Role of Prosocial Emotions in Motivating Action for Social Change."</a> <a href="http://psr.sagepub.com/content/13/4/310.short">http://psr.sagepub.com/content/13/4/310.short</a> > These Australian social scientists provide an extensive review of the literature on

- Evidence that membership in groups can support prosocial
   <a href="http://learningtogive.org/papers/paper52.html">http://learningtogive.org/papers/paper52.html</a> > outcomes ("helping behavior, altruism, cooperation, and solidarity");
- Factors supporting prosociality in groups
- The roles of emotion (specifically guilt, sympathy and outrage) in fostering prosocial outcomes.

The authors' focus is on prompting action for social change in support of disadvantaged groups; however, there are implications for our work in encouraging employees to pay attention to security in their organizations.

One of the key findings of research on prosociality in the last four decades discussed by the authors is that "there are three core processes that underpin prosocial group behavior: category inclusion, category norms, and category interests."

• Category inclusion refers to how people see themselves as members of defined and inclusive groups. Thus if employees see themselves as belonging to "the company" or

"the organization" rather than solely as members of a smaller subgroup ("technical support" or "accounting") they may respond more favourably to attempts to stimulate prosocial behaviour such as identifying and reporting violations of security policy. Note that there is no conflict in belonging to both a sub-group and the more inclusive group; the issue is whether a person sees any common identity with the larger group.

- Category norms refers to expected or normative behaviours for a group. These norms are explicit articulations of values; for example, "We really ought to report a stranger who is walking about in a restricted area" could be a category norm for the security team; the challenge is to extend this norm to the wider class of all employees.
- Category interests are "the strategic concerns that accompany helping behavior." For example, convincing employees that their own personal reputations and the reputation of the entire company are threatened by security breaches would be a development of a category interest.

Emotion plays an important role in moving people towards concerted action (social *action*). The authors point out two ways that emotion can lead to social action:

- Identification as a member of a distinct group can lead to shared (group) emotion shared feelings (positive or negative) about issues which in turn can lead to social action.
- Individual emotions can lead people into identifying themselves with social groups and again, lead to social action.

In our security context, perhaps we can build on these two sequences. For example, fostering group identity using such tools as, say, t-shirts with a company logo or motto (with or without additional subgroup individuation such as the addition of, say, "tech support" or "security team") or by hosting social events to which all members of the organization are invited (as opposed to having only members of a specific department attend) could solidify group identity. The other approach would involve articulation of group values that could attract employees into self-identification with the social identity. In my experience, for example, Hewlett-Packard (HP) in the 1980s was successful in fostering a set of shared values, starting with "People are our number 1 resource." I have often told students about how, in 1982, a recession decreased sales significantly for HP worldwide; upper management circulated an announcement to all HP offices worldwide starting that the company had to cut salary expenses by 10% -- but instead of firing 10% of the 87,000 employees at that time, they reduced everyone's salary by 10% and offered us all every second Friday off as an unpaid holiday. In the office where I worked (#2012 in Kirkland, Quebec), not one employee quit – and no one took the free Fridays, either. Instead, we worked like blazes to serve our customers (I was a systems engineer in the HP3000 group at that time) and to advance our internal training. By 1983, when the economy turned back up, we were 'way ahead of our main competitors, who had to scramble to hire and train new employees. In those years, HP consistently won J. D. Powers awards for customer service.

In terms of category inclusion, the authors write, "groups' emotions have the potential to shape and restructure (inter)group boundaries. For example, experiencing feelings of fear in relation to another person is unlikely to lead to a categorization of that person as an in-group member...." In contrast, several lines of research support the view that when people share the same emotions, they may strengthen their group identification. In the security context, perhaps we can articulate the legitimate threat from criminal hackers, industrial spies, and attackers sponsored by nation-states to strengthen dislike of these out-groups among our employees. I am not proposing exaggeration and propaganda here: providing accurate descriptions of the depredations of these

attackers should suffice to support increased group identification and therefore increased willingness to take action in defence of the group.

The authors review work by several scientists suggesting that "anger plays a powerful role in politicizing a social identity, transforming the identity such that it is more ready for social action." Perhaps more explicit reference to the cultures and threats of the attackers could have positive outcomes in solidifying group identify among our employees and supporting active responses in support of information security. For example, expressing anger at organized cybercrime syndicates<

http://money.cnn.com/2011/07/27/technology/organized\_cybercrime/index.htm > such as the Russian Business Network (RBN)<

http://www.spamhaus.org/rokso/evidence/ROK7740/russian-business-network/media-a-walk-on-the-dark-side > that was active during the mid-2000s<

http://www.spamhaus.org/rokso/evidence/ROK7740/russian-business-network/media-a-walk-on-the-dark-side >. Providing educational material detailing current attackers' behaviour and emphasizing that we are justified in expressing anger at their illegal actions may be a positive contribution to encouraging more prosociality to support increased vigilance and readier reporting of clues to suspicious activity on our systems.

Research into category interests supports the view that "emotions will shape the sorts of strategies that group members prefer... in particular depending on where the emotion implies that blame lies (one of the key appraisal categories...)." So perhaps in our security briefings, a bit more visible outrage about the culture and bad behaviour of our attackers may actually contribute to reinforcing the willingness of our colleagues to engage in better defences. Instead of maintaining a detached objectivity about cyberscum (!), we may be better off letting our indignation show through during training and awareness sessions.

Other sections of the authors' article cover details of prosocial emotions (guilt, sympathy, and moral outrage) and also of self-focused anger as factors affecting prosociality. Some of the key findings of particular relevance to information security are as follows:

- Guilt refers to feelings of responsibility for behaviour or situations which are viewed as negative, harmful, wrong or immoral. Interestingly, "it is possible to induce guilt in people even though their personal self was not responsible for the harm inflicted on another." Perhaps a security trainer who expresses regret over the loss of reputation experienced by a victim of q stolen password lost by responding to a phishing e-mail can parlay this sense of responsibility into a group acceptance of an evolving moral norm: it is "wrong" (not just silly or careless) to be unaware of common techniques for identity theft. However, guilt is not viewed as a powerful motivator of prosocial behaviour; indeed, "there are at least three ways that individuals can avoid the experience of group-based guilt: They can minimize the harm that was done to the other group, question the appropriateness of guilt, and engage in argument about the cost of apology...."
- Sympathy is "heightened awareness of another's plight as something to be alleviated...." Sympathy seems to be a strong motivator for both "interpersonal...and intergroup prosocial behavior...." Perhaps focusing on the personal consequences of specific or typical victims of breaches of security (e.g., suspicion cast on an innocent victim of password theft) could support behaviours to reduce the occurrence of such security breaches. However, it seems to me that it would be unwise to express sympathy for cybercriminals, regardless of their motivations.<

http://www.cyberwarzone.com/cyberwarfare/pinoy-hackers-scale-attacks-china-websites

• *Empathy*, distinct from sympathy, is a move towards increased identification with the other; thus in our context of information security, awareness and training sessions my benefit from emphasizing the commonality of all victims of cybercrime. Instead of feeling bad for other people, an empathic response would move employees to see themselves as potential victims. Perhaps we could explicitly engage in role-playing to encourage our colleagues to articulate how they would feel as the victims of various cybercrimes.

The paper has much more of interest for those of us working on security awareness and training, and I recommend it highly.

Those with access to academic libraries will find it easy to locate paper or electronic versions of the article at no cost to them. However, the publisher does make the article available as a downloadable PDF – for the usual exorbitant fee (in this case, U\$25), illustrating as always the notable commitment of commercial publishers to the advance of human knowledge – by receiving articles without payment to the authors, receiving scholarly reviews of the manuscripts without payment to the reviewers, and asserting exclusive ownership of the published articles.

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

## **Blunt Advice for Freshmen**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Recently I responded to a journalist's requests for top suggestions on what college students should know about information technology and security. Here are my responses. Pass them on to kids you know.

So you're going to college in a month? Here are some brutal observations about your use of information technology.

- 1) Securing your information as you head to college involves six fundamental aspects of information:
- a) Confidentiality think about \_who\_ should know \_what\_ about you. Do you really want to post pictures of yourself apparently breaking the law (e.g., through under-age alcohol consumption) so that anyone including non-friends, professors, and potential employers have access to the pictures?
- b) Control once you reveal information, who will be able to use it without your permission? Kids who use sexting and send their "friends" nude pictures of themselves can discover those pictures sent all around a complete circle of strangers as the original recipient boasts or his or her sexual conquest. If you send a terrible e-mail full of anger at someone else (like a teacher), how do you know it won't be distributed without your permission and cause real problems for everyone?
- c) Integrity if you forward crap about the end of the world or how eating potato chips with ketchup will kill you to your friends without actually checking to see if the info is correct (e.g., by consulting SNOPES.COM), what do you think your reputation will be like when the truth comes out? And if you write or spread lies about named people, did you know you could be sued for libel? How's that going to look on your resume?
- d) Authenticity hmm, your buddies want to use your computer and you let them sign on as you! So what happens when they send a "joke" to the White House using your name and threat to kill the President? I'll tell you what happens: you get a visit from the Secret Service within a few hours. Don't EVER let someone use your identity for ANYTHING!
- e) Availability my dog may not have eaten my homework, but my computer crashed and wiped out my essay. Yeah, right. We professors hear it all the time but we always ask, "So where are your backups?" Backups copies taken at different times preferably with different version numbers on your homework files can not only save your ass when your disk drive crashes, they can even prove that YOU wrote the essay your roommate just STOLE and presented as her own work, resulting in an accusation of plagiarism against YOU.
- f) Utility make sure you check with your profs about how they want electronic work submitted. It's not going to do you a bit of good to send in a PDF document if the prof explicitly

asked for only DOCX, DOC, RTF or ODT files.

- 2) A computer virus / worm / Trojan can ruin your whole day or academic term. Always be sure that your computers, notebooks, tablets, and phones are running adequate antimalware software. It's just part of the cost of running those devices get over it.
- 3) Total strangers who claim in an e-mail that they are sexually attracted to you or have millions of stolen dollars they want to give to you as a commission on money transfers are LYING. The ones telling you that they can cure cancer, change body parts to enormous sizes, instantly improve your sex appeal, and give you thousands of dollars a week for very little work that you can do from home are LYING. Don't get fooled. Use a spam filter for your e-mail and remember what you've heard for years: if it sounds too good to be true, it's probably not true.
- 4) In the USA and some other countries, making, sending or downloading child pornography is a federal crime. That also means that making, sending or storing nude pictures of underage children using your cell phone is a federal crime. DON'T BE STUPID.
- 5) Kids are dying in road accidents and many of them are found to have been typing text messages on their phones while they were driving. Although you may think that they deserve Darwin Awards for removing themselves from the gene pool, actually they just have underdeveloped prefrontal cortex and so do you. That means that kids often lack judgement about the risks involved in their chosen behaviour, especially if "everybody else" or "the cool kids" are going it. So keep your head literally. Text while driving and you have an excellent chance of dying or ending up paraplegic, quadriplegic, or brain-damaged. Sorry kids, it's time to grow up.

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

Copyright © 2012 M. E. Kabay. All rights reserved.

# A Canticle for TinyURL: Electronic Information in a Post-Apocalyptic World

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Starting around 300 BCE, the pharaohs of Egypt built a library at Alexandria, Egypt to house a growing collection of mostly Greek texts. By the time of its destruction in 391 CE by frenzied early Christians who, like the religious fanatics of today<
http://online.wsj.com/article/SB10001424052702303292204577519052197927504.html?mod=googlenews\_wsj.>, felt threatened by anything other than their own narrow concepts of acceptable culture, it had become one of the greatest repository of human knowledge in the world.<
http://www.britannica.com/EBchecked/topic/14417/Library-of-Alexandria.> Its destruction was a significant milestone in the descent into the half-millennium-long dark ages of Europe, North Africa and the Middle-East.< http://www.britannica.com/EBchecked/topic/151663/Dark-Ages.> For an entertaining and moving fictional representation of the time of the destruction of the Library at Alexandria, see the 2009 movie "Agora,"< http://www.imdb.com/title/tt1186830/.>, which tells the story of the famous scholar Hypatia.
http://www.britannica.com/EBchecked/topic/279463/Hypatia.>

I want to jump now to an award-winning science-fiction story published in 1960: A Canticle for *Leibowitz* < http://www.amazon.com/Canticle-Leibowitz-Walter-Miller-Jr/dp/0060892994/ > by Walter M. Miller, Jr. < http://www.enotes.com/walter-m-miller-jr-salem/walter-m-miller-jr > The book opens in the 26<sup>th</sup> century CE after the mid-20<sup>th</sup>-century nuclear holocaust of this timeline has effectively destroyed technological civilization. In a rage against the scientists and technicians they view as responsible for unleashing the atomic disaster on the world, hordes of maddened zealots destroy every sign of nuclear technology, then of high technology, then of all books, then of literacy itself. Calling themselves "Simpletons" in scorn for the educated and the literate (much like today's right-wing ideologues who sneer at "elites" < http://www.youtube.com/watch?v=K4-vEwD\_7Hk > when referring to anyone who seems marginally more intelligent than Sarah Palin< http://www.youtube.com/watch?v=W J0fIF8x10 >)(sorry, couldn't resist), these descendants of the survivors sink into a new dark age. By the 2600s, the Roman Catholic Church persists as the key organization devoted to finding, preserving, and hand-copying every remaining book – or indeed, any scrap of writing at all – that the priests, monks and acolytes can find. One of the funnier passages has a novice on a Lenten fast discovering a trove of written material from the much revered engineer Leibowitz, who is the patron figure for his religious order (and is being considered for beatification); he finds a cryptic set of words that he and others could view has having potentially great spiritual significance. It's actually a grocery-shopping list.

I've been thinking about what might happen to our own global culture if we hit another period of destruction – say, mass migrations of starving people moving from insufferably hot and dry regions of the world into more polar lands with different cultures and language. What if civilization lost electric power? Would the Internet persist? And if it didn't, what would the consequences be for the preservation of human knowledge and culture?

E-books and electronic versions of newspapers, magazines and journals are growing in popularity. In 1998, Professor Eli Noam< <a href="http://www.citi.columbia.edu/elinoam/">http://www.citi.columbia.edu/elinoam/</a> of the Business School at Columbia University published a thoughtful analysis of the changing role of paper books in education. "Electronics and the Decline of Books: The Transformation of the Classroom"</a> <a href="http://net.educause.edu/ir/library/pdf/ffp9807.pdf">http://net.educause.edu/ir/library/pdf/ffp9807.pdf</a> on editor wrote, "It is characteristic of individuals, institutions, industries, and entire societies to misjudge the future. They do so by simultaneously exaggerating, belittling and fighting change.... The future of books and the university is being similarly misunderstood.... [I]nescapably, books as a physical entity eventually will become a secondary tool in academia, their role usurped by electronic media. The firms associated with books, publishers, will decline, and the role of the university will change dramatically." In the latter version, Noam suggests that there are four types of books in use in academia:

- "texts, as source material for analysis
- textbooks, for instruction
- scholarly monographs and edited volumes, for dissemination of research and broader discussion
- academic journals, also for dissemination of research."

After summarizing a number of trends pushing information into the electronic versions of such materials, Noam concludes,

"These trends add up to a significant shift away from books in academia, the inner sanctum of the book culture.... Books are yesterday's technology. Those in academia, who love books, lament their decline. But is it not *knowledge* that we really cherish, and aren't books merely the receptacle? A new and creative medium is knocking at the door, one that should be embraced."

Steve Coffman< <a href="http://www.lssi.com/leadership.html#">http://www.lssi.com/leadership.html#</a> of Library Systems and Services<
<a href="http://www.lssi.com/index.cfm">http://www.lssi.com/index.cfm</a> published an extensive "paper" (the irony!) in April 2012
called "The Decline and Fall of the Library Empire."<
<a href="http://www.infotoday.com/searcher/apr12/Coffman--The-Decline-and-Fall-of-the-Library-Empire.shtml">http://www.infotoday.com/searcher/apr12/Coffman--The-Decline-and-Fall-of-the-Library-Empire.shtml</a> > He notes that public-access computing — the availability of computer terminals at public libraries — has increased radically since the invention of the World Wide Web:

"Today, nearly 100% of all public libraries offer public internet access. The number of public access PCs has gone from almost nothing in the early 1990s to nearly 100,000 in 2000, and by 2009 – the latest IMLS data available – that number had more than doubled to 232,505. So, during the past 20 years, public internet access has grown into a mainstay of public library service. .... [T]he evidence indicates that public internet access is a valuable service and that the public has flocked to take advantage of it. A 2010 study by the Gates Foundation showed that more than 77 million people – or nearly a third of the entire U.S. population – were using libraries to access the internet and doing it for all manner of reasons – keeping up with friends via social sites or email, doing homework, filling out job applications, researching employers, and all those other activities we engage in on the internet. Many of these people would not have been able to engage in those activities without the public internet PCs at their local public library."

Coffman points to another trend – the growing use of e-books:

"Certainly there can be no doubt that ebooks have caught on with the general public. Amazon and Barnes & Noble have both reported more ebooks are being sold than paper books. The growth in the ebook market has been so strong, it's led some publishing pundits such as Mike Shatzkin to predict that an 80% ebook world for straight narrative text is coming in 2 to 5 years<
http://www.idealoa.com/bloq > .... Whether you agree with those sorts of wild predictions or not, there is a ... consensus in the publishing industry that the ebook era has definitely arrived and has already begun changing the way books are produced, sold, and read in some pretty fundamental ways....

[S]ome of the libraries that offer ebooks have reported large increases in circulation. For example, Seattle Public Library claims its ebook circulation jumped by 92% in 2010; New York Public says it increased 81% in 2011; and the Kansas State Library reported a tenfold increase in ebook circulation between 2006 and 2010, leading to a 700% increase in its OverDrive<a href="http://www.overdrive.com/">http://www.overdrive.com/</a> > bill."

In the UK, there's evidence of growing e-book usage as well. Professor David Nichols< <a href="http://www.ucl.ac.uk/news/news-articles/1001/10010802">http://www.ucl.ac.uk/news/news-articles/1001/10010802</a> > of the School of Library, Archive and Information Studies, University College London and several colleagues published a survey in 2008 of "UK scholarly e-book usage...."<

http://www.emeraldinsight.com/journals.htm?articleid=1733496 > involving 22,437 responses from over 120 institutions were analysed. They concluded that "e-book penetration is very strong (61.8 per cent of all students are already [2008] using them in connection with their scholarly work, as teachers or students), so the e-book revolution has already happened but clearly it has some way to go."

For a case-study of how a breakdown in availability to an electronic data source can compromise access to knowledge, consider the uniform resource locator (URL) shortening services. These tools are particularly useful for Twitter messages because of the 140 character limit; a long URL can easily exceed that limit. They are also helpful in e-mail, where long URLs may be folded (and broken) by automatic formatting in the e-mail clients.

Tinyurl reports "over a billion" abbreviated URLs and vaguely claims "billions of redirects per month." < <a href="http://tinyurl.com/">http://tinyurl.com/</a> > Bitly, which is now the standard abbreviator for URLs in Twitter messages < <a href="http://techcrunch.com/2009/05/06/url-shortening-wars-twitter-ditches-tinyurl-for-bitly/">http://techcrunch.com/2009/05/06/url-shortening-wars-twitter-ditches-tinyurl-for-bitly/</a> >, responded to a request for information with the following data:

- "Close to 100 million links saved per day
- Over 25 billion bitly links created thus far
- 300 million clicks on links per day [and thus around nine billion clicks per month]
- Microsoft Research estimates bitly sees 1 percent of all clicks on the Internet."

These large databases of electronic abbreviations are an example of wholly electronic data storage and access. What happens if the organization running a shortening service goes out of business or decides to terminate its service? That actually happened to trim (tr.im), which gave

up its unsuccessful competition with bitly at the end of 2009<
<a href="http://mashable.com/2009/08/09/trim-shuts-down/">http://mashable.com/2009/08/09/trim-shuts-down/</a> >. All references using solely the tr.im abbreviated URLs were useless – were lost – from that point on.

I think that the potential inaccessibility of abbreviated URLs if there is widespread infrastructure disruption should make us think about the evanescence of other forms of solely-electronic information storage. Because my wife and I live in a rural area of Vermont in the USA, we've had a standalone emergency electrical generator since we moved to our home in July 1998; so do our relatives and many of our friends. We can continue to access the Internet even if mains power fails.

Just today as I write this, I learned that my brilliant octogenarian aunt's Internet service has been unavailable for unknown reasons for the last four days and won't be restored for at least another three days. She notes with dismay that e-mail and Web access have become integral tools for her; being without them is a noticeable stress.

What are we going to do if the entire electrical grid fails and the servers of the Web are no longer running? The venerable *Encyclopedia Britannica* stopped printing book versions of the great work in 2010 after 244 years of continuous publication.<

<a href="http://money.cnn.com/2012/03/13/technology/encyclopedia-britannica-books/index.htm">http://money.cnn.com/2012/03/13/technology/encyclopedia-britannica-books/index.htm</a> > So how will children who use the electronic version of the *Encyclopedia Britannica*<

<a href="http://www.britannica.com/">http://www.britannica.com/</a> > manage to complete their school essays without access to their familiar store of information?

I don't think we're yet at the stage where complete inaccessibility of the Internet would destroy any hope of rebuilding society, but the more information we store electronically on workstations and servers or on devices (CD-ROMs, DVDs, Blueray discs) requiring electronic access, the more vulnerable we will become.

What is society to do if an entire generation of people find themselves forced to return to using paper documents – decades after the last libraries abandoned their physical books and journals?

Will electronic data storage be seen as a component of a millennium-long dark age when scholars of the 31<sup>st</sup> century look back on their history?

\* \* \*

As always, comments are most welcome. Sincere thanks to Fiona Tang for the quick response about bitly usage volumes.

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

## **Consultants**

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

In 1986, I submitted my first essay to the magazine of INTEREX, the HP3000 user community. Perhaps it will interest readers to decide whether my suggestions are still useful more than 25 years later. I updated the article in 2004 and 2007 and now to correct modified (or disappeared) Web references. For more old essays, see "Computer Envy: Essays on Office Automation." <a href="http://www.mekabay.com/opsmgmt/envy.pdf">http://www.mekabay.com/opsmgmt/envy.pdf</a> >

Office automation (OA) can be approached from two sides. For administrative services, OA is the introduction of tools developed originally in data processing (DP) to the office. From DP's angle, OA is the extension of "normal" methods to every wider fields of application. Because few of us have expertise in both spheres, a good deal of money is spent on external consultants who help bridge the gap between DP and OA.

Here are some guidelines to help both DP and OA staff extract every penny of value from their investment in consultants.

How much consulting gets done in industry as a whole? Globally, several tens of thousands of individuals and thousands of firms bill several billion dollars a year for services in general management, financial management, marketing, production, data processing, personnel, and small business administration. You can get information on sources of consulting by

- contacting your hardware and software vendor representatives and describing the sort of problem you are concerned about;
- speaking to members of your professional associations, including local and international computer users' groups for references to well thought of firms;
- contacting trade associations.

#### Scope

When the client and consultant are discussing OA problems and how the consultant could help, both parties must be conscious that a consultant always has two allegiances: to the manager hiring her and to the firm employing the manager. You must define the scope of the consulting assignment so that the consultant can in fact legitimately tackle the task. For example, it would be pointless for a local OA manager to request assistance in deciding whether to implement satellite link teleconferencing nationwide within a corporation. Such a project would be beyond the manager's scope.

Sometimes consultants are asked by managers to produce support for a predefined set of conclusions as part of an internal political battle; consultants should be chary of accepting such assignments without making it clear that their report may very well disagree with preconceptions.

As you evaluate potential consultants, look for those who can state their understanding of your problems clearly. I am fond of the phrase, "Let me see if I have understood" because it's a

chance to test my perceptions against those of the client. When you have chosen your consultant, prepare an action plan that defines what you both plan to do, by when and how you will know when to stop.

All consulting is aimed at change: either fixing what doesn't work or improving what already does or inventing a new solution for a problem foreseen. By writing down what will constitute sufficient change, you ensure that your external consultant does not become an unwanted permanent member of your corporate family. A consultant is not a permanent employee of your department. A reasonable expectation is that with time, the frequency of consultant visits will decline for any specific project. As part of the assignment, consultants normally expect to work closely with members of the client organization to impart their knowledge and methods.

Consulting fundamentally involves teaching. I once met a consultant who did minicomputer performance analysis. I asked him what tools he taught his clients to use in analysing system performance; he answered, "Tools? I don't teach any tools. Listen, if a client is going to spend thousands of dollars on a performance monitor, I'd rather he spend it on me." Clients must ask their consultant exactly how their firm will become less dependent on external help by paying for consulting time.

A professional consultant will clearly identify the limits of her knowledge. Faced with requests for help in areas beyond his competence, the consultant will point out that alternative sources of information would be more cost effective. One test you can apply to judge the professionalism of a prospective consultant is to ask her to identify the limits of her professional competence.

#### **Ethics**

The International Labour Organisation (ILO) had a useful code of ethics for consultants but it seems to have disappeared from the Web. [Anyone finding it is invited to post the current location in our comments section.]

The codes of professional conduct are basic instruments used by the consultants' associations to establish the profession and protect its integrity.... Thus members of the associations engage themselves

- To place the client's interest ahead of their own;
- To keep information about the client confidential and take no advantage of its knowledge;
- To accept no commissions in connection with the supply of services to the client;
- To hold no directorship or controlling interest in any business competitor of the client without disclosing it;
- Not to invite an employee of a client to consider or apply for suggested alternative employment;
- Not to calculate remuneration on any other basis than a fixed fee agreed in advance, which may be on a time rate;
- To inform clients of any relationship and interest that might influence the consultant's judgement;
- To accept no assignment which exceeds the scope of their competence;
- Not to work when their judgement might be impaired by illness, misfortune or any other cause:
- To refrain from seeking business by public advertising or by payment of commission for

the introduction to clients.

For good measure, you can also think about the Code of Ethics < <a href="https://www.isc2.org/ethics/default.aspx">https://www.isc2.org/ethics/default.aspx</a> > of the (ISC)<sup>2</sup>, the certifying authority for Certified Information Systems Security Professionals, which comprises the following admonitions:

#### Code of Ethics Preamble:

- Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this Code is a condition of certification.

#### Code of Ethics Canons:

- Protect society, the commonwealth, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

Everyone will benefit from consideration of these principles when choosing consultants and when delivering consulting services.

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

Copyright © 1986, 2007, 2012 M. E. Kabay. All rights reserved.

## The Expert in the Next Office

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Ah, summertime, when the typing is easy. I'm posting a few of my favourite essays published over the last quarter century. This essay was first published in 1988 (note the reference to Lotus 1-2-3, an early and hugely popular spreadsheet) in the Interact "Office Automation" column and again in 2000 in the Network World Security Strategies column. It remains one of my favourites after all these years — and I believe that the lessons still apply.

"Marcie, can you spare a minute?" Marcie groans inwardly. This is the sixth time this morning someone has come in from a neighbouring office to ask her for "a minute". Each occasion lasted about a quarter of an hour. The questions all concerned LOTUS 1-2-3, on which Marcie is the acknowledged expert.

However, Marcie is actually the Assistant to the Director of Finance, not a Technical Support specialist from the Information Centre in Data Processing. Every time she's interrupted by a call for help from people in Accounting, Shipping, Engineering, and even occasionally from Data Processing, she falls further behind in her assigned work. She likes helping people, but lately she's had to stay late after the nominal end of her work day simply to make up for the time she has used acting as informal technical support to her neighbours.

Marcie may have a bad time of it unless something changes in her organization. She may be fired by her boss because her productivity drops too low according to her job description. She may burn out and quit because of overwork and criticism. Or she may cause resentment among her colleagues and neighbours by declining to help them or by complaining to her own boss and causing a ruckus. Alternatively, she may have a good time and manage to meet all the demands on her quite successfully until the DP department begins to feel threatened and someone either complains to the higher ups or begins spreading nasty comments about poor, helpful Marcie. Being the expert in the next office is tough on the expert.

Looking at this situation from a management point of view, there are problems for the recipients of all this free aid. The longer they can persist in getting apparently free help from their unofficial benefactor, the longer they can avoid letting upper management know they need help with their office automation tools. Then when the bubble bursts and the expert becomes unavailable, managers are confronted with a sudden demand for unplanned resources. In some organizations, unexpected staffing requirements are difficult to satisfy. Managers have a hard time explaining how it is that they were unable to predict the need and budget for it.

#### **TINSTAAFL**

Engineers often say, "There is no such thing as a free lunch" (abbreviated TINSTAAFL) to imply that no benefit is without cost.

From a technical support perspective, even the most gifted unofficial expert is necessarily an amateur. True, there are many users whose technical knowledge of their tools exceeds that of their own technical support staff. But professional technical support consists of far more than just technical knowledge. Almost no amateur expert will

- Have colleagues to discuss the problem with on a technical level;
- Have backup personnel so she can provide faster service to requesters;
- Search the appropriate technical manuals with the user experiencing a problem;
- Have access to all the periodical information provided by manufacturers;
- Document the problems carefully so as to avoid having to solve them all over again later;
- Have access to phone in consulting services;
- Determine the cause of the problem and ensure that the problem does not recur; and
- Broadcast information about the problem, its workaround, and its fix to unaffected users who may benefit from the information.

### **Summary**

In conclusion, it is more sensible for employees to help themselves and each other by letting management know they need technical support. When someone asks you for technical help, by all means help them – but let your manager know immediately that there's a support problem. When you have a technical problem yourself, by all means ask your expert neighbour for help if it's a matter of seconds to solve it – but tell your own manager that it was an exceptional case and that you'd much rather have a permanent technical support team to work with.

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

Copyright © 1988, 2000, 2012 M. E. Kabay. All rights reserved.

## Internet Addiction & the Central-Limit Theorem

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Do you ever think that your electronic communications devices are getting a little bit intrusive? At a performance of "God of Carnage"<

http://youtube.googleapis.com/v/HIInXwGU6Ww&amp > presented by Lost Nation Theater,
http://lostnationtheater.org/info/ > the local regional theatre in central Vermont (USA), one of the characters enrages everyone else at an evening meeting in a home by interrupting the serious discussions to answer his mobile phone. How many times have you interrupted a serious discussion at work or an intimate moment with your loved one(s) to answer a phone, tablet, notebook or tower computer's imperious summons?

Internet addiction< <a href="http://www.netaddiction.com/">http://www.netaddiction.com/</a> > is a separate issue from what I think of as Internet-mediated attention deficit syndrome. A recent article by Tracy McVeigh< <a href="http://www.guardian.co.uk/profile/tracymcveigh">http://www.guardian.co.uk/profile/tracymcveigh</a> > in the Guardian/Observer (which, ironically, I read using a Kindle program on a tablet computer) reported that "Internet addiction even worries Silicon Valley: Experts warn of the addictive power of technology"</a> <a href="http://www.guardian.co.uk/technology/2012/jul/29/internet-addiction-hooked-digital-technology">http://www.guardian.co.uk/technology/2012/jul/29/internet-addiction-hooked-digital-technology</a> >. The journalist writes, "...attention is shifting from compulsive surfing to the effects of the all-pervasive demands that our phones, laptops, tablets and computers are making on us."

Mike Elgan< http://www.computerworld.com/s/author/9000162/Mike+Elgan > discussed the distracting power of "a world of amusements ... always just a click away" in a Computerworld article in March 2011<

http://www.computerworld.com/s/article/9215078/Elgan\_How\_to\_overcome\_Internet\_distraction\_n\_disorder >. He notes that spending time on distractions such as social-networking sites, online games, movie reviews and shopping can result in an *impression* of having done a lot of work; however, the key question is "What did I accomplish?" Alas, he writes, "For many, the honest answer is: 'Not very much.'" Worse, "...as Internet distractions gobble up more of our time and attention, we feel like we're working harder while our real work keeps piling up. So we force ourselves to work more and longer hours and bring more of our work home. The more we work, the more our minds rebel and gravitate to the amusements. It's a self-reinforcing phenomenon that results in not really enjoying fun, and not getting our work done."

Elgan suggests that one helpful approach to reduce distractions is the segregate work on specific devices and strictly observe the difference. Don't play games or visit Facebook on your office computer; don't read business e-mail on your mobile phone. Personally, I have used this approach for many years; for example, I do forward my phone to my mobile phone when I'm out of my home office – thus providing a single phone number for everyone – but I disconnect the autoforward at the end of the work day and turn off my phone when I go home.

The prevalence of instant communications has changed our conception of appropriate speed of communication. In my childhood (the 1950s) and youth (1960s), people routinely sent *correspondence on paper* via the mails; turnaround time could be a week for a simple written

communication. Naturally, we used telephones, but only Star Trek had portable communicators< <a href="http://www.youtube.com/watch?v=MNF5lvB0Q0k">http://www.youtube.com/watch?v=MNF5lvB0Q0k</a> > resembling today's mobile phones. The first mobile-phone call was in 1973 – and the phone weighed a kilogram.<
a href="http://fc05.deviantart.net/fs45/f/2009/122/e/3/DynaTAC\_8000X\_versao\_2\_by\_denuxo.jpg">http://fc05.deviantart.net/fs45/f/2009/122/e/3/DynaTAC\_8000X\_versao\_2\_by\_denuxo.jpg</a> >

For many years, as a professor of statistics<

http://www.mekabay.com/courses/academic/norwich/qm213/index.htm >, I've explained to students that the central-limit theorem< http://www.khanacademy.org/math/statistics/v/central-limit-theorem > has real-world applications. One form of the theorem is that, in the absence of additional information, any random event will most likely be average. Thus if we receive a phone call, we can expect that the call will be of average importance. The key is that if we consider what we're doing to be *more* important than average, *we should not answer the phone*. If what we're doing is *less* important than average, *answer the phone*. Now, the judgement of importance of the phone call can be improved by knowing who is calling or whether one has asked for a return call on a critical issue; the principle remains: don't interrupt your current activity unless you decide that the interruption has a higher importance to you than what you are doing.

I don't answer business calls after the day is over – I want to spend time with my wife, not continue interacting with business associates and students, no matter how nice they are. Recently I phoned a colleague on the West coast of the US and discovered that he was having lunch with fiancée, who lives in British Columbia. I told her to slap him upside the head for interrupting his lunch with her and told him *never* to put a phone call higher in priority than his time with his fiancée.

Should you have your e-mail client online while you are working? Once again, ask yourself whether what you are currently working on is more important or less important that average. If you are on a higher-priority task, don't look at your e-mail until later. And don't think that just because someone sends you an e-mail, you must respond immediately.

What if you know that some e-mails may in fact be high priority? You would like to see and respond to e-mails from a colleague who needs information urgently on a project or from your supervisor who may have priority-changing instructions for you. OK: use your e-mail client's functions for filing incoming e-mail according to sender, to subject, or even to specific keywords in the body of the message. File those in a folder called PRIORITY or IMPORTANT or URGENT and leave your e-mail client focused on that one, not on the general in-basket.

What about the "Important" flag available in many e-mail systems? It can be helpful, but only if everyone in your workgroup or circle agrees on guidelines for its use. For example, marking a message *important* may be justified if there is an urgent response required (and you will have to agree on what *urgent* means, too). However, if members of your group start applying the *important* flag to the most recent joke or for invitations to tennis games after work, the system will collapse into a mass of useless messages, all marked *important* – and you will be back to an undifferentiated mass of e-mail.

One final note: even if you notice a text message, instant message, e-mail message or voice-mail message, you do not have to respond immediately. Don't let the ease of communications become an imperious demand for response. Set your own priorities as you see fit and don't let other people's well-meaning interruptions deflect your from your purpose.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

Copyright © 2012 M. E. Kabay. All rights reserved.

# Pulling Back the Blinders: Extending IT Security to Physical Threats

Ryk Edelstein & M. E. Kabay

Ryk Edelstein< <a href="http://ca.linkedin.com/in/ryked">http://ca.linkedin.com/in/ryked</a> > is CEO of Cicada Security<<a href="http://www.cicadasecurity.com">http://www.cicadasecurity.com</a> > and has served as CEO and lead developer of their Cicada active physical-security technology. What follows is the result of a close collaboration between Ryk and Mich.

\* \* \*

#### Introduction

The focus of information technology (IT) security practitioners in recent decades has been to secure data systems from unauthorized access and corruption caused by an ever-growing range of logical threats – compromise through the layers of the Open Systems Interconnect (OSI) model.< http://support.microsoft.com/kb/103884 > We implement security measures to protect the back office and the data communications infrastructure through to the client station against known and potential software-based exploits.< http://nvd.nist.gov/ > However, despite the costs and efforts to protect against virtual threats, it seems to me that we expend little effort to protect these systems from physical threats such as theft or tampering A report< http:// www.iofm.com/content/resources/OverallSecuritySpending1.pdf > published in 2011 by the Institute of Finance & Management < http://www.iofm.com > reported on wide differences in spending on physical security within and across industries, with significant proportions of the respondents spending less than 1% of their total budget on physical security. Although many executives reported that they felt that their organization's spending on physical security was adequate, "At the other end of the spectrum, a majority of security executives working in health care facilities, government, and retail feel the amount that is spent on physical security is insufficient to deliver quality asset protection."[p 5]

In the decades when mainframe computers were the norm, physical security.<a href="http://searchsecurity.techtarget.com/definition/physical-security">http://searchsecurity.techtarget.com/definition/physical-security</a> was immediately recognized as a critical element of IT security. For example, the third edition of the *Computer Security Handbook* published by Wiley in 1995 included explicit sections about physical security; for example,

- Chapter 11: "Hardware Elements of Security"
- Chapter 12 "Computer Facility Protection"
- Appendix 3: "Security Standards Manual Table of Contents (Sample)" which includes 10 headings about physical facility security out of 49 section headings
- Appendix 14: "Federal Information Processing Standards: Abstracts" which points to FIPS PUB 31, "Guidelines for ADP Physical Security and Risk Management" dated June 1974

An industry standard compilation of security policies – Charles Cresson Woods' *Information Security Policies Made Easy*< <a href="http://www.informationshield.com/ispmemain.htm">http://www.informationshield.com/ispmemain.htm</a> > emphasizes the importance of physical-security policies:

#### 7.01.01 Physical Security Perimeter

#### 2. Physical Security Plan

Policy: Every Company X data center must have a physical security plan that is reviewed and updated annually by the senior manager in charge of the facility.

Commentary: This policy explicitly assigns responsibility for the development and updating of data center physical security plans. This policy makes it clear that physical security is a line management responsibility, not a staff department responsibility. This means that physical security must be dealt with in the course of ordinary data center operations, not exclusively by a special group. A special technical group, ordinarily called the Physical Security Department, is generally available for consulting and assistance. In most cases the senior manager in charge of the data center would not actually prepare the plan. Somebody else who reports to the senior manager will typically do this. Some organizations may wish to include words in the policy indicating that this plan will be subject to periodic review by the Internal Audit Department. Good physical security must be in place if good information security is going to be achieved. For example, if anybody off the street can walk into a data center and reboot a machine, then load their own version of the operating system, much if not all of the good work in the information security area will be null and void.

Related Policies: "Critical Business Logic" and "Computer Emergency Response Plans."

Audience: Management

Security Environments: All

#### **Today's Environment**

It's hard to secure a laptop, tablet or smart phone that is outside the corporate offices. Encryption, host intrusion prevention, and other end point security technologies are important but they cannot reliably protect a device that is powered on, unattended and unprotected from theft, unauthorized access and tampering. These end-point platforms don't afford the administrator ways of protecting external devices from physical threat.

There are solutions with limited applicability to the general problem of supporting physical security of portable devices. For example, several products provide the ability to encrypt whole disks or to wipe or reset mobile phones, tablets and notebook computers through network connections if their owners report them as lost or stolen:

However, these products suffer from fundamental inadequacies:

- Whole disk encryption provides no benefit to the protection of the data stored on these devices when the device is active, since the encryption works automatically as soon as the authorized users logs on.
- Asset-recovery services, although valuable, are typically invoked only once the owner of the computer has *discovered* the loss or theft. If a service provider can be alerted the moment the event occurs, the system can start tracking sooner and invoke policy-based actions for the protection, transfer, and destruction of data stored on the target asset.
- Physical restraint products cannot ensure usage compliance and cannot report attempted theft or tampering. In any case, they are barely a challenge for a motivated thief.

With federated-identification < <a href="http://www.federatedbusiness.org/index.php/faqs">http://www.opengroup.org/security/sso/</a> > strategies playing a greater role in securing our distributed networks, we need to audit and enforce physical security on all connecting stations the moment a threat is detected.

The *Cicada*, from Cicada Security Technology, my Montreal-based company, has been engineered to expand security visibility to the physical level. This patented technology, which was originally designed to provide active protection against asset theft, has proven itself to also be a valuable solution for the protection of any station which hosts confidential information or connects to a secure trusted environment. No larger than a common USB flash storage device, the Cicada is capable of analyzing inputs from a number of trigger sources, and when triggered, instantly invokes both deterrent and protective actions to secure its host station. Triggers include motion, device insertion or removal, insertion of writable media, power and network state changes, amongst other options.

As I recently wrote< <a href="http://cicadasecurity.com/blog/2012/07/expanding-the-vision-of-security-the-importance-of-gaining-visibility-to-physical-threat/">http://cicadasecurity.com/blog/2012/07/expanding-the-vision-of-security-the-importance-of-gaining-visibility-to-physical-threat/</a>>,

Once triggered, the Cicada invokes user defined protective actions which can include locking the host to the operating login screen, activating a siren on both the device and the host, dismounting an encrypted volume, and in more extreme cases, brick the host, or even destroy cryptographic keys. As can be imagined, as the protective action occurs the moment the threat is detected, and any information stored on, or is accessible from the active host is instantly protected, and the possibility of exposure of confidential information is minimized.

When deployed as an enabling technology, end-point security platforms make physical threats noticeable and are able to invoke actions defined in their own policies, thus extending their effectiveness to protect the enterprise. At the gateway, authentication policy can be extended to require the presence of an active physical-security device meeting specific policy requirements before the host can be granted access to the trusted environment.

In the case of the Cicada, each device has an embedded indelible serial number which can be used as a secondary authentication factor, enabling the assigned user to be able to roam while carrying both a secondary authentication factor and their physical security technology from station to station. Likewise, as a required component to the authentication process, usage compliance is assured.

The Cicada has been launched for sale with its active monitoring and alerting service. It is currently a participant in the Government of Canada's (GoC's) Canadian Innovation Commercialization program< <a href="https://buyandsell.gc.ca/initiatives-and-programs/canadian-innovation-commercialization-program">https://buyandsell.gc.ca/initiatives-and-programs/canadian-innovation-commercialization-program</a> > and is being evaluated by GoC departments.

For more information about the Cicada, see our Website<
<a href="http://www.cicadasecurity.com/?p=products">http://www.cicadasecurity.com/?p=products</a> > and feel free to contact me personally at any time</a> <a href="mailto:ryk@cicadasecurity.com">mailto:ryk@cicadasecurity.com</a> >.

\* \* \*

Ryk Edelstein< mailto:ryk@cicadasecurity.com > has been actively involved as the CEO of IT networking and security-services companies for over 30 years. He is currently the lead developer and CEO of Cicada Security Technology< <a href="http://www.cicadasecurity.com/">http://www.cicadasecurity.com/</a> >, a Montreal, Quebec based developer of innovative security technologies engineered to protect assets and data against the risk of physical threat. He has been responsible for providing guidance to both public and private sector clients on the protection of their digital assets, and is the co-author of the guide titled "Best Practices for the Destruction of Digital Data" <a href="http://www.amazon.com/dp/B008UZHQA4">http://www.amazon.com/dp/B008UZHQA4</a> which addresses current and validated data handling practices for the decommissioning of end-of-life storage hardware using properly aligned technologies.

[Disclaimer: M. E. Kabay has no involvement in or financial interest in the Cicada product or Cicada Security Technology.]

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

\* \* \*

Copyright © 2012 Ryk Edelstein & M. E. Kabay. All rights reserved.

## Taking Professional IA Certifications to a New Level: Interview with Rolf Moulton

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Rolf Moulton, CISSP-ISSMP < <a href="http://www.linkedin.com/pub/rolf-moulton-cissp-issmp/0/170/811">http://www.linkedin.com/pub/rolf-moulton-cissp-issmp/0/170/811</a> > has a long and distinguished career in information assurance. He is running for office to resume his role as a Board Member for the International Information Systems Security

Certification Consortium, Inc., [(ISC)^2] < <a href="https://www.isc2.org/cgi/content.cgi?category=12">https://www.isc2.org/cgi/content.cgi?category=12</a> > and I was so interested by his proposals that I invited him to respond to some questions.

Everything that follows is Rolf's own work with minor edits.

\* \* \*

Rolf, what prompted your interest in information assurance (IA) from the start?

People and process. Information security was a great way to work with people throughout an organization. This was obvious to me in each of my CISO positions (Unilever, BP America & Department of Investigation). I was very fortunate to be a member of I4 (The International Information Integrity Institute) during the 1980s, and later with the ISF (Information Security Forum). Participation in these groups, as well as in many conferences and discussions, led me to the conclusion that realistic guidelines, discipline and structure, as well as both sympathetic empathy and a bit of humor, were needed to move the practice of information security forward. And that we, as information security practitioners, would benefit by defining repeatable processes to establish what needed to be done, why it mattered, what risk, cost and resource trade-offs were available to define the "what if we do" and "what if we don't" areas of opportunity, and to then get the job done. There also needed to be a way to differentiate between those people who had a sufficiently reasonable understanding of how to manage the process from those who were not yet ready to do it. So, I was already a believer in the need to establish practitioner/professional certification when I was asked to participate in the (ISC)^2 startup.

When and how did you become involved in the International Information Systems Security Certification Consortium, Inc., (ISC)^2?< <a href="https://www.isc2.org/cgi/content.cgi?category=12">https://www.isc2.org/cgi/content.cgi?category=12</a>>

I became involved in (ISC)^2 in 1990 when (ISC)^2 invited me to participate in the Waiver of Formal Examination (Grandfathering) Committee. The importance of the start-up of (ISC)^2 and its potential ability to provide the means to deliver both a solid credential and an enforceable code of ethics for information security practitioners (professionals) was clear – and that it would take a lot of work by many people to get it going. The credential and code of ethics, together with the continuing education requirement, could serve as the basis to start turning the information security art form into a profession.

I moved to the UK to lead the Unilever Corporate Information Security Program and was away from direct (ISC)^2 involvement for a while. Then I was invited to join the (ISC)^2 Board to fill a vacancy and was elected to the Board. While serving on the Board, the PCEO (President and Chief Executive Officer – who is the paid professional manager of the (ISC)^2 support

operation) retired and a temporary PCEO was needed while a new PCEO was selected. So, I resigned from the Board and took this "temporary" assignment, which lasted 18 months. After this wonderful and unique opportunity to work directly with the membership and the operations staff ended, I was elected back onto the Board. I left the Board when the Bylaws' term limits required that I take a break in my service. I am now standing for (re)election to the (ISC)^2 Board as an "Independent eCandidate."

In your view, how have the certifications programs of (ISC)^2 helped professionals, the practice of information assurance, and the world?

The CISSP, as the first (ISC)^2 certification, really got the ball rolling as the benchmark credential for defining the criteria for a reasonably knowledgeable and experienced information security professional. I personally saw it as a fundamental certification. It defined what employers should look for in hiring and/or promoting an information security professional, as well as the basis for defining parts of some academic curricula. This was a very important achievement because many practitioners could not clearly define and substantiate what they knew and understood; there also needed to be a code of ethical conduct and a requirement for continuing education. This has changed with the success and maturity of the CISSP and the certification. CISSP now also addresses areas of professional competency. For many, having an (ISC)^2 certification is a requirement for getting hired or staying in a position. The above have also influenced the hiring and promotion practices for many information security/assurance professionals internationally.

Where do you see the Consortium moving forward in the coming decade?

That will depend on what the membership and the marketplace demand and what the Board hears and delivers. I believe that there are four key areas that should be addressed as (ISC)^2 moves forward.

1. **Certification:** This is the core of what (ISC)^2 offers and there are more than 83,000 active CISSPs, as well as a smaller number of (ISC)^2 certifications that include CSSLP, SSCP and CAP. There also seem to be too many different "certifications" that are currently being offered by too many providers. This is confusing the marketplace; some rationalization is needed. There will continue to be a need for current technology practitioner *competency certificates* in contrast to *professional certifications*, such as the CISSP and the other (ISC)^2 certifications.

The CISSP (Advanced Level) (CISSPAL), which I have proposed, has the potential to be developed as the CISSP <u>plus</u> a demonstration of experience and/or accomplishments. Preparing the specifics for a detailed proposal of what would define "Advanced Level" will take a good bit of research and negotiation. (ISC)^2 would benefit by collaborating with groups who have been working on this approach, such as the IISP in the UK.

The CISSPAL was intended as a thought provoking <u>preliminary proposal</u>. It is very apparent from various discussions and correspondence that it is a controversial proposal. There have been strong diverse opinions:

- (1) Some CISSPs have advised that a CISSPAL is long overdue and could help to establish a professional progression;
- (2) Some have argued that now is not the time to tinker with anything that might relate to their current job or getting the next job;

- (3) Others don't see the need for a change and consider this to be a needless exercise rather than an effort to advance the profession;
- (4) Many others have been silent and may be waiting to see what may or may not be developed and proposed by the (ISC)<sup>2</sup> Board.

Clearly, a very thorough needs analysis and business case will be necessary before concluding that this is the right or the wrong approach to take at this time.

There is the potential for changes that may be suggested or required by governments and governmental agencies. Certifications have been required by some companies, governments and governmental agencies as mandatory to secure or hold a specific job. It is also not clear how this may evolve with regard to licensure in the future.

I would greatly appreciate comments and suggestions from readers sent to me< <a href="mailto:rolf.moulton@boardcandidate.com">mailto:rolf.moulton@boardcandidate.com</a> > about the need for or opposition to the preliminary proposal for the CISSPAL.

- 2. Education: Education has been a cornerstone service for (ISC)^2. In my opinion,
  - Providing education services will continue although the delivery mechanism(s) should be reviewed to provide and expand the content more easily and at a lower cost:
  - Likewise, the ability to respond to changes more quickly needs to be addressed;
  - Conferences and seminars, individually and jointly with other providers, both live and virtual, have been very successful and need to continue to be developed and offered in a wider range of formats and venues.
- 3. **Professional development and support:** This is an important opportunity that needs to be explored more to determine what should be done as a professional support institution and what will be demanded by the Membership by virtue of Member participation and support. The chapter program, which I helped to initiate as part of the ALIG (Affiliated Local Interest Group) program, is part of this professional development support initiative that needs attention, with a very strong emphasis on cooperation with and support of related chapter organizations. Additionally, we worked with the ISF to get a better understanding of how to help "the next generation" of InfoSec professionals and then created the "career path" approach; this also needs more development and attention.
- 4. **Community Outreach:** The (ISC)^2 Foundation is a fairly new initiative. It will play a key role going forward as a means to provide service and support to the public, industry and the future for information use and protection. This will continue to be an area of continued growth that can look to providing education and policy level support on critical issues related to information and infrastructure protection.

With Rolf's permission, here's the letter he sent out to several hundred (ISC)^2 members during August, 2012.

Subject: With more than 83,000 CISSPs, when do we get an "Advanced Level" CISSP?

There are now more than 83,000 active CISSP certificate holders. The wide variations in the certificate holders' experience levels are not reflected in the current "fundamental" CISSP

certification or the confusing concentrations: CISSP-ISSAP, CISSP-ISSEP and CISSP-ISSMP. This puts Advanced Level CISSPs at a recognition and a negotiating disadvantage. It also does not provide the right professional growth incentive for less experienced CISSPs.

I am taking the liberty of sending my recommended CISSP upgrade actions for the (ISC)^2 Board to you because I believe that you are concerned about protecting the value of your CISSP certification. And, because I need your help for me to bring a business case for creating the Advanced Level CISSP to the Board as an "Independent" Board Member....

To create the CISSPAL, the "Advanced Level" CISSP, I believe that the (ISC)^2 Board needs to:

- Clarify what each of (ISC)<sup>2</sup>'s certifications represents today,
- Perform a rigorous Membership and marketplace review and evaluation of all (ISC)^2 and other InfoSec certifications that are currently planned or available including those for cloud, mobile, CND....,
- Upgrade/Create those (ISC)^2 certification(s) and related professional support that are needed,
- Implement the right marketing and support program to communicate the benefits of the CISSPAL to all CISSPs, as well as to the business and technical managers who hire and promote CISSPs.

I ask that you please sign the Petition to add my name as an "Independent Candidate" to the (ISC)^2 Board Election Ballot now by replying to this e-mail and including your (ISC)^2 Member (Certificate) Number. Or complete the Petition Form on the Board Candidate Website.<a href="http://www.boardcandidate.com">http://www.boardcandidate.com</a>

Then, if I am elected to the Board later this year, I can work as part of the Board to start making the priority changes that are needed to create the CISSPAL certification, as well as consider the possibly of Advanced Levels for all of the other (ISC)^2 certifications.

Thank you in advance for your consideration, help, and support – and I hope for signing my petition.

Regards,

Rolf Moulton, CISSP-ISSMP

(ISC)^2 Board of Directors Candidate

E-mail: mailto:rolf.moulton@boardcandidate.com

Website: <a href="http://www.boardcandidate.com">http://www.boardcandidate.com</a>

[Disclaimer: The opinions presented in this interview are those of Rolf Moulton, who is not currently an (ISC)^2 Board member, and they do not represent those of (ISC)^2 or the Board of (ISC)^2.]

Rolf Moulton< <a href="mailto:rolf.moulton@boardcandidate.com">mailto:rolf.moulton@boardcandidate.com</a> has served as President and CEO (Interim) of (ISC)^2and as an (ISC)^2 Board member. Currently, he is a Director at Risk Reduction Solutions. Previously, he served as Head of IT Risk Management and Information Security at Unilever, IT Security Manager at BP America and as Director of the Computer Security Services Unit at the Department of Investigation (NYC). He holds the CISSP-ISSMP certification and MBA and BA degrees and is an active member of Information Systems Security Association (ISSA)<a href="http://www.issa.org/">http://www.issa.org/</a> >. He helped to initiate the (ISC)^2 Chapter program, was a founding ISSA Chapter President, and was an active participant in the development of the Institute of Information Security Professionals (IISP) in the UK. He has authored many professional articles, a security management textbook<a href="http://www.amazon.com/Computer-Security-Handbook-Strategies-Techniques/dp/0131658042/">http://www.amazon.com/Computer-Security-Handbook-Strategies-Techniques/dp/0131658042/</a> >, and was a participating developer of BS7799 and ISO17779.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2012 Rolf Moulton & M. E. Kabay. All rights reserved.

# Layers of Meaning: Free Statistics Textbook

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Why should information assurance (IA) professionals care about applied statistics?

One reason is that distinguishing between chance variations and unusual anomalies can lead system, network and security administrators to problems that might be discovered much later, when they approach disaster status. In "Pay Attention to Anomalies," I pointed out the operational consequences of a software failure that ignored interruption of automatic payments by members of a health club. In the article, I showed a familiar diagram illustrating the *change in slope* or *inflection point* in a growth curve as a possible indication that something has changed in the operational processes about which we are concerned.

But how do we tell if something is *significant* or merely a minor chance variation?

Decision under uncertainty is one of the descriptions of applied statistics, although it's hard to know who said that first. Making decisions when the facts don't allow a clear-cut decision among alternatives is difficult; it's easy to decide to cross a street when there are no cars visible at all, but the moment cars are in sight there are questions of how fast they are going, whether pedestrians are *likely* to be visible, whether the drivers are *likely* to be insane sociopaths who want to run over pedestrians, and so on. Admittedly, one could push the example to ridiculous extremes, such as arguing that we have to weigh how *likely* it is that the street will cave in just as pedestrians step out onto the pavement, whether a meteor is *more likely* to strike a pedestrian crossing the street than a pedestrian standing on the sidewalk, and so on.

All of these questions imply that absolute certainty is impossible; we are victims of randomness and have to cope with uncertainty as best we can. Look at all the cases where italics highlight "likely;" we take uncertainty for granted in the real world and generally cope with it intuitively, without having to use statistical methods explicitly or consciously.

Applied statistics includes an area called *hypothesis testing* that deals specifically with evaluating the *likelihood* that a particular model of external reality – that a particular model of external reality – the *hypothesis* – is *consistent* with *unbiased* observations. For example, turning back to network security, we might say that we hypothesize that the rate of attacks on our gateway security devices today is consistent – not from expectation – with recent attack rates. So if we expect 200,000 attacks a day on our IP addresses and today we see 300,000, does that increase mean that someone new is attacking our systems, or that old adversaries are focusing on us – or is it just the luck of the draw?

Answering the question is beyond the scope of this column, but intuitively, a lot depends on how *variable* our historical data are. For example, if the number of attacks ranges from, say, 150,000 to 250,000 over the last month, a value of 300,000 might not be a clear indication of a real

change. But if the attack rates vary from 190,000 to 210,000 for the last 30 days, maybe a value of 300,000 is something to make admins' eyebrows go up.

This column is not intended to teach anyone details of statistical methodology: it is a pointer to a new version of a statistics textbook I've been working on since 2010. Now in its fourth prepublication version ("v0.4"), *Statistics in Business, Finance, Management and Information Technology: A Layered Introduction with Excel*<

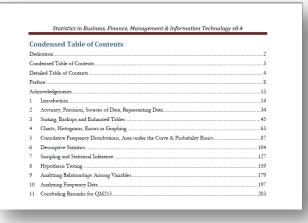
http://www.mekabay.com/courses/academic/norwich/qm213/statistics\_text.pdf > is a 200-page introduction to practical applications of statistics for estimation and hypothesis testing. The material is the basis for my QM213 "Business & Economic Statistics I" course< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > at Norwich University< http://www.norwich.edu > and is freely available to all users. My only requests are that no one post copies online (in public or on intranets); simply point to the file instead – that way when I make corrections, everyone will have access to the latest version. And naturally, I would be very cross indeed if anyone *sells* what I *give away free*!

The text provides practical guidance on using Excel 2010 for routine statistical processing; more important, I put a lot of work into explaining the underlying reasoning for all these methods. This is a book for practitioners and should allow users to improve their understanding of *which* statistical methods to use *when*.

The short-form table of contents will give readers a sense of the topic areas.

The structure of the text is unusual in that topics are introduced several times, helping readers and students get used to why various methods are used before they are introduced to how to carry out the computations.

I will be grateful to readers who point out errors or possible improvements in the text – this project is definitely run under the standards of continuous process improvement.



Have fun (assuming having fun and statistics are not mutually exclusive for you).

\* \* \*

For a primer about applied statistics aimed at IA professionals, see "Understanding Computer Crime Studies and Statistics, v6" which became chapter 10 in Bosworth, S., M. E. Kabay, & E. Whyne (2009), eds. *Computer Security Handbook*, 5th Edition. Wiley (ISBN 978-0471716525). 2 volumes, 2040 pp. AMAZON < <a href="http://www.amazon.com/Computer-Security-Handbook-Volume-Set/dp/0471716529/">http://www.amazon.com/Computer-Security-Handbook-Volume-Set/dp/0471716529/</a> >

\* \* \*

M. E. Kabay,< <u>mailto:mekabay@gmail.com</u> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information

Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< <a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2012 M. E. Kabay. All rights reserved.

## **Mining for Gold in ISTS Resources**

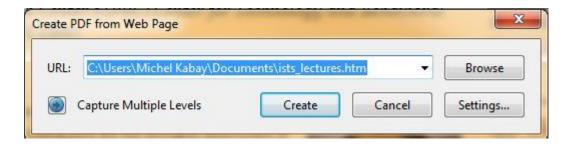
by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

The Institute for Security, Technology, and Society (ISTS)<
<a href="http://www.ists.dartmouth.edu/about/">http://www.ists.dartmouth.edu/about/</a> was founded in 2000 at Dartmouth College in Hanover<
<a href="http://www.hanoverchamber.org/">http://www.hanoverchamber.org/</a> >, New Hampshire<<a href="http://www.visitnh.gov/">http://www.visitnh.gov/</a> >, USA. ISTS is explicitly dedicated to three interlocking goals (quoting directly from their self-description):

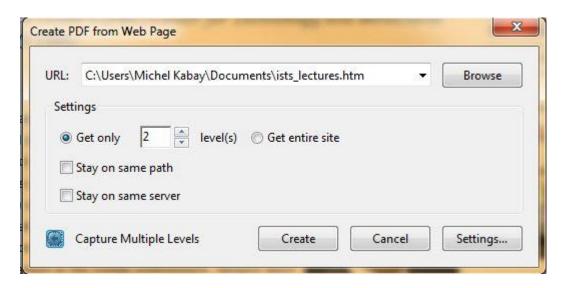
- RESEARCH, to extend knowledge and provide insight and innovation in the area of information security
- EDUCATION, to increase the number of students and faculty involved in technology research, and to increase community awareness of privacy and security challenges and solutions related to IT
- OUTREACH, through collaborations that deploy technology and encourage knowledge transfer for both public and private benefit.

One of the valuable resources offered to information assurance (IA) educators is the extensive series of lectures< <a href="http://www.ists.dartmouth.edu/events/">http://www.ists.dartmouth.edu/events/</a> > by stimulating thinkers in the field. Many of these have been recorded< <a href="http://www.ists.dartmouth.edu/events/#Video lectures and panel discussions">http://www.ists.dartmouth.edu/events/#Video lectures and panel discussions</a> > and provide excellent opportunities for professionals engaged in self-directed learning and for teachers and students in IA classes, whether in higher education or in industry.

Not wishing to click on link after link and wait for the screen to refresh – my Internet access in rural Vermont maxes out at 2.8 Mbps (yes, bits, not Bytes) – I used a tool that surprisingly few of my students and even colleagues know about: getting Acrobat Professional (not the Reader) to download all the pages linked to an HTML page and creating a single PDF file from them. I captured the HTML code for all the summary pages, pasted them into a document, and saved it as an HTML file. Then Acrobat Professional used the Create | PDF from Web Page < file:052\_acrobat\_menu\_1.jpg >



with a two-level capture < file:052\_acrobat\_menu\_2.jpg >



that generated a 312 page catalog!

Browsing at my ease, here are (only) *some* of the exciting lectures specifically relating to IA that I found in this treasure trove of goodies.

- 2012-04-26: Gary McGraw < <a href="http://www.cigital.com/~gem/talks/#bio">http://www.cigital.com/~gem/talks/#bio</a> > "Cyber War, Cyber Peace, Stones, and Glass Houses." <a href="http://www.youtube.com/watch?v=LCULzMa7iqs">http://www.youtube.com/watch?v=LCULzMa7iqs</a> > The distinguished scientist argues that "...[T]oo much of the discussion about cyber security is ill informed, and even sophisticated policymakers struggle to sort hype from reality. As a result, Washington focuses on many of the wrong things. Offense overshadows defense. National security concerns dominate the discussion even though most costs of insecurity are borne by civilians. Meanwhile, effective but technical measures like security engineering and building secure software are overlooked."
- 2012-04-04: Anita Allen< <a href="https://www.law.upenn.edu/cf/faculty/aallen/">https://www.law.upenn.edu/cf/faculty/aallen/</a> > -- "Privacy in the Era of Social Media: Goodbye to Health Privacy."</a> <a href="http://www.youtube.com/watch?v=vd-CDkvp83g">http://www.youtube.com/watch?v=vd-CDkvp83g</a> > The Henry R. Silverman Professor of Law and Professor of Philosophy at the University of Pennsylvania discussed the wideranging implications of the generational and radical changes in the concepts of privacy that we are currently experiencing.
- 2011-11-11: John Halamka
   <a href="http://connects.catalyst.harvard.edu/profiles/profile/person/46034">http://connects.catalyst.harvard.edu/profiles/profile/person/46034</a> -- "Information Security in Healthcare what's keeping me up at night in FY12."
   <a href="http://www.dhslides2.org/informatics/informatics111111f/f.htm">http://www.dhslides2.org/informatics/informatics111111f/f.htm</a> > Dr Halamka was Chief Information Officer for the Harvard Medical School in July 2011
   <a href="http://www.informationweek.com/healthcare/leadership/halamka-to-leave-harvard-med-school-cio/231002441">http://www.informationweek.com/healthcare/leadership/halamka-to-leave-harvard-med-school-cio/231002441</a> > With his wealth of first-hand knowledge of IA in the medical field, he analysed key IA issues for US hospitals and doctors, with direct applicability to the medical field worldwide.
- 2010-10-06: Steven Davis< <a href="http://www.linkedin.com/in/playnoevil">http://www.linkedin.com/in/playnoevil</a> > -- "Protecting Computer Games and Entertainment Security."<
  <a href="http://www.youtube.com/watch?v=inKABNzNpH4">http://www.youtube.com/watch?v=inKABNzNpH4</a> > As CEO of a firm specializing on

- the computer-game and gambling industries, Mr Davis shed light on an obscure area with surprisingly extensive security issues.
- 2009-11-12: Neel Sundaresan< <a href="http://labs.ebay.com/neelsundaresan/">http://labs.ebay.com/neelsundaresan/</a> > -- "'Are People Basically Good?' An Interweaving Story of Trust, Commerce, and Technology at the Long Tail."<a href="http://www.youtube.com/watch?v=ZvLY\_201khg">http://www.youtube.com/watch?v=ZvLY\_201khg</a> > The Senior Director and Head of the eBay Research Labs reviewed "technical, economic, and social aspects" of social interactions through eBay.
- 2009-10-13: Andrew Cutts< <a href="http://www.ccdcoe.org/cyberwarfare/162.html">http://www.ccdcoe.org/cyberwarfare/162.html</a> > -"Cybersecurity Policy: Keeping the Broad View."<
  <a href="http://www.youtube.com/watch?v=V6EQwV9lEKE">http://www.youtube.com/watch?v=V6EQwV9lEKE</a> > The Director of Cyber Security Policy at the US Department of Homeland Security reviewed his work in "...supporting the national cyber initiative, developing cybersecurity strategies, advancing the understanding of national cyber risk, clarifying roles and missions, and helping operational efforts mature."
- 2009-05-04: Jonathan Zittrain<
   <a href="http://www.law.harvard.edu/faculty/directory/index.html?id=106">http://www.law.harvard.edu/faculty/directory/index.html?id=106</a> -- "Civic Technologies and the Future of the Internet."<
   <a href="http://www.youtube.com/watch?v=couon3Ge9ug">http://www.youtube.com/watch?v=couon3Ge9ug</a> > The celebrated thinker and author considers the "design, development and deployment of cutting-edge technology for information security and privacy, all the while attending to the social and economic aspects of new technologies in society and their implications for security and privacy."—Introduction by Professor Denise Anthony</a>
  <a href="http://www.dartmouth.edu/~socy/faculty/anthony.html">http://www.dartmouth.edu/~socy/faculty/anthony.html</a> >, Research Director of the ISTS.

Readers will find a wealth of excellent materials among these resources. Congratulations to the ISTS staff and their guests!

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2012 M. E. Kabay. All rights reserved.

# Trends in the Threat Landscape: Joshua Rosenthal at the eCampus Security 2012 Conference

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

The annual Securing the eCampus conferences< <a href="http://www.ists.dartmouth.edu/events/ecampus/">http://www.ists.dartmouth.edu/events/ecampus/</a> > are a valuable and enjoyable opportunity for security experts interested in security at educational institutions. Organized by staff of the Institute for Security, Technology, and Society (ISTS)</a> <a href="http://www.ists.dartmouth.edu/about/">http://www.ists.dartmouth.edu/about/</a> >, these conferences have been hosted at Dartmouth College in Hanover</a> <a href="http://www.hanoverchamber.org/">http://www.visitnh.gov/</a> > since 2007.

This year Joshua Rosenthol< <a href="http://www.ists.dartmouth.edu/events/ecampus/bios/rosenthol.html">http://www.ists.dartmouth.edu/events/ecampus/bios/rosenthol.html</a> >,CISSP of Websense Labs< <a href="http://securitylabs.websense.com/">http://securitylabs.websense.com/</a> > presented an excellent overview< <a href="http://www.ists.dartmouth.edu/docs/ecampus/2012/2012ecampus\_rosenthol.pdf">http://www.ists.dartmouth.edu/docs/ecampus/2012/2012ecampus\_rosenthol.pdf</a> > of the changing Internet threat landscape.

Websense Labs reported on current Adobe Reader vulnerabilities. Key exploits include

- Blackhole 1.1.0 < <a href="http://malwareint.blogspot.com/2011/08/black-hole-exploits-kit-110-inside.html">http://malwareint.blogspot.com/2011/08/black-hole-exploits-kit-110-inside.html</a>
- Phoenix 2.0, 2.3-2.5, 2.7< <a href="http://malwareint.blogspot.com/2011/10/inside-phoenix-exploits-kit-28-mini.html">http://malwareint.blogspot.com/2011/10/inside-phoenix-exploits-kit-28-mini.html</a> >
- Crimepack 2.2.1, 2.2.8, 3.0.0< <a href="http://www.inreverse.net/?p=1401">http://www.inreverse.net/?p=1401</a>>
- Bleeding Life 2.0< <a href="http://krebsonsecurity.com/2011/01/exploit-packs-run-on-java-juice/#more-6876">http://krebsonsecurity.com/2011/01/exploit-packs-run-on-java-juice/#more-6876</a>>
- Impassioned Framework 1.0< <a href="http://krebsonsecurity.com/2010/07/pirate-bay-hack-exposes-user-booty/#more-3337">http://krebsonsecurity.com/2010/07/pirate-bay-hack-exposes-user-booty/#more-3337</a>>
- Katrin Exploit Pack< <a href="http://cyb3rsleuth.blogspot.com/2011/05/katrin-exploit-pack.html">http://cyb3rsleuth.blogspot.com/2011/05/katrin-exploit-pack.html</a> >.

One startling statistic is that if users apply patches immediately when they are released, they nonetheless suffer 104 days of exposure! The speaker quoted an IDC *Threat Intelligence Update* from 2012-02-14< <a href="http://www.idc.com/getdoc.jsp?containerId=prUS23290912">http://www.idc.com/getdoc.jsp?containerId=prUS23290912</a> > that found that "Signature based tools (anti-virus, firewalls, and intrusion prevention) are only effective against 30-50% of current security threats. Moreover, customers expect the effectiveness of signature-based security to continue to decline rapidly."

Websense Labs characterize the Web threat lifecycle into the following stages:

- Lure: social-engineering tricks such as YouTube scams, gift offers, natural-disaster relief appeals, targeted spam, and e-mail about specific events and alerts, fake surveys, blog postings (Oh no! Say it ain't so!);
- Redirect: concealing the actual destination of links;
- Exploit Kit: malicious programming to exploit holes in Adobe products, Java, browsers and even TrueType fonts;

- Dropper File: fake antivirus programs, malicious apps, browser plugins;
- Call-Home and Data Theft: data transfer applications that copy and transmit confidential data, including password files.

Websense Labs' ThreatSeeker Network< <a href="http://www.websense.com/content/ThreatSeeker.aspx">http://www.websense.com/content/ThreatSeeker.aspx</a> relies on "the world's first Inernet HoneyGrid." This system "...is a network of technology and human intelligence that creates an adaptive feedback network that uses more than 50 million real-time data collecting systems to parse one billion pieces of content daily.

The presentation closed with the following ranked predictions for 2012:

- 1. Social Media accounts and targeted attacks
- 2. Mobile attacks
- 3. SSL traffic creating blind spot
- 4. Containment is new prevention
- 5. London Olympics, US Presidential Election.

I'll finish with my own recommendations for everyone:

- Be on your guard: do not open e-mail from strangers casually.
- Have your antimalware and antiphishing tools online and up to date at all times.
- Convert HTML e-mail to ASCII automatically.
- Verify that the address of a link matches the label for the link exactly.
- Be suspicious of links in top-level domains you don't normally interact with; e.g., if you never have e-mail from Russia or business in France, don't click on a link to URL in .RU or in .FR without careful consideration.
- Block e-mail encoded in languages you do not speak; e.g., if you don't speak Chinese, reject e-mail from .CN.

The full *Websense 2012 Threat Report*< <a href="http://www.websense.com/content/websense-2012-threat-report-download.aspx">http://www.websense.com/content/websense-2012-threat-report-download.aspx</a> is available free with simple registration.

My thanks to Joshua Rosenthol for his informative lecture and to ISTS for inviting him to speak.

\* \* \*

[Disclaimer: M. E. Kabay has no relationship whatever with Websense (except for appreciating their research and publications) or with ISTS (except for enjoying their conferences, their publications and their wonderful staff).]

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2012 M. E. Kabay. All rights reserved.

## **Kitty Porn**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

A few weeks ago my wife and I looked for a Russian Blue kitten we could adopt. We found an ad on the "kittensforadoption.us" site with a picture of a cute kitty available in Massachusetts, a few hours' drive from our home in Vermont.



We contacted the owner using the REPLY function. We quickly got a nice e-mail from "Susan Haper" cheerfully telling us

"Greetings from this end and i'm glad to read back from you. As i said, we have three available 1 male and two female and they are purebred Russian blues. They are 13 weeks old respectively, The male is called Paige and the females are called Shannon and Jessy.i am glad that you want to take one of them." [All the errors are in the original message.]

I received a phone call a day later by a man with a thick African accent who said he was the husband of "Mrs Susan." I had to return his call, so I used the number I saw on my mobile phone, 385.200.1409. While I was speaking with him on a bad line, another African man interrupted the conversation, which was almost incomprehensible. The caller kept insisting that he wanted my wife's e-mail address, even though she had already received an e-mail response as shown above.

Then we received the following astonishing news: the "Massachusetts" kitties were in Salt Lake City, Utah – more than 3000 km away!

"hi after reading your mail, i was over whelm and wanted no body else to have this my baby except your loving family for they are perfect

match to siamese.

they are 4 months old and i am located in salt lake city Utah and i have both male and female of the baby. i will advice since you are a cat lover to take both the male and female to you.

i can them ship to you there in vermont and it is not the first time i will be doing that so you dont have to worry.

also attached to this email are the pics of the male and female. like i said they are for adoption and all you have to pay is for the shipping to you and before sending you this email i had to talk to the agency and they told me it will cost you 380\$ for both male and female to be home deliver to you from Utah to Vermont.

they will be needing the following from you: full name, contact number and nearest airport to your location (that is if you will receive them at the airport)

but if you will like for them to be deliver to your home address then you have to add: city and postal code, street name and home address.

originally i had 4 babies as you will see and only the two single photos i am sending of the male and female are left."

At this point, my alarm for "advance-fee fraud" went off and I looked into the situation in detail.

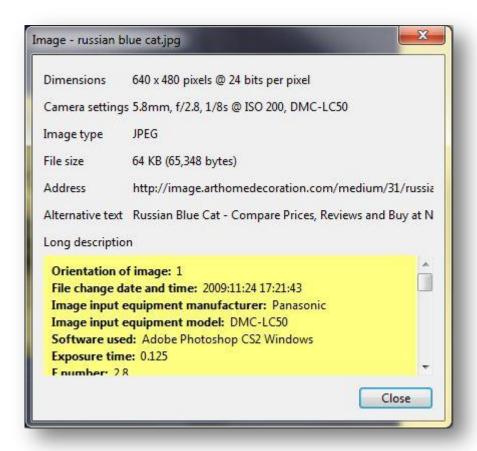
#### Here are my key findings:

- The phone number (385.200.1409) has over 6,000 hits on Google (try it yourself) for every imaginable kind of animal including wild animals that cannot legally be raised or traded in the USA and animals covered under the Convention on International Traffic in Endangered Species (CITES< <a href="http://www.cites.org/">http://www.cites.org/</a>>.
- Analysis of the first thousand Google hits for ads using the 385.200.1409 phone number showed that almost all of them were on sites registered outside the USA.

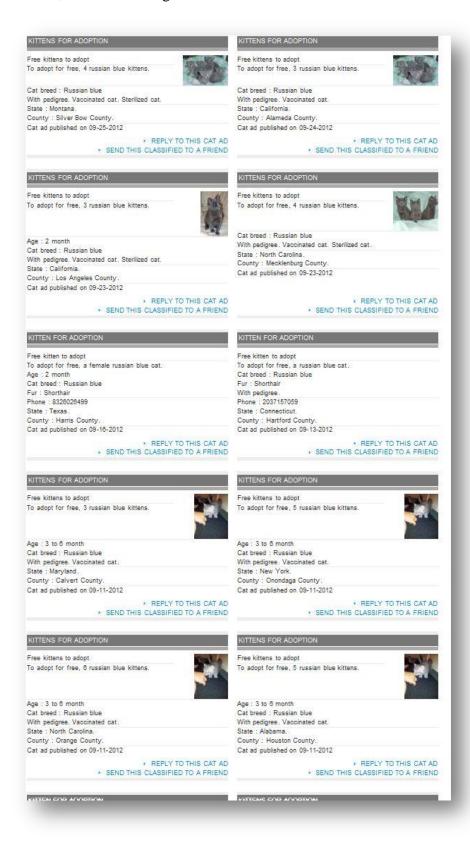
Website	Domain registered in
www.adtob.com	Romania
www.animalssale.com	Ukraine
www.bedfordshire-central-bedfordshire.adtob.com	Romania
www.juneau.adtob.com	Romania
www.kittensforadoption.us	Germany
www.little-rock.adtob.com	Romania
www.usaphonestore.org	Australia
www.usmarketdb.com	USA

• Exactly the same description of the kittens ("With pedigree. Vaccinated cat. Sterilized cat.") generated 5,620,000 hits on the kittensforadoption.us Website *alone*.

• The picture of the nice cat on a blue background was quick to find using Google Images using the search string < russian blue kitten > and turned out to be from a picture gallery < <a href="http://image.arthomedecoration.com/medium/31/russian%20blue%20cat.jpg">http://image.arthomedecoration.com/medium/31/russian%20blue%20cat.jpg</a> >; clicking on "Image Properties" showed that it was from 2009 or earlier.



- Examination of the same page where the original "Massachusetts" kitty was posted showed dozens of cases< <a href="file:054\_3\_lots\_of\_copies">file:054\_3\_lots\_of\_copies</a> > of identical photographs used for different cats in widely separated areas of the US.
- Using the Neustar domain registration service< <a href="http://www.whois.us/">http://www.whois.us/</a>>, we found that the kittensforadoption.us Web site was registered by a German company supposedly by someone living in Beverly Hills, California. The phone number of the registrant, 213.631.1402, is not a working number.



The pattern fits that of the *advance-fee fraud*< <a href="http://affcoalition.org/">http://affcoalition.org/</a>>, also known as the 4-1-9 Nigerian Fraud (a reference to the Nigerian penal code section covering this kind of crime) in which a sucker is cajoled into believing that (s)he will get something for nothing. The scammers then announce that a fee is required for completion. The request for "shipping" costs for nonexistent cats (unless someone has figured out how to clone the critters) is a giveaway. Had we sent money, we would almost certainly have been told that another, even higher fee was required for completion of the transaction.

We should have been suspicious the moment we determined that the expensive Russian blue purebred kittens were *free* – and included three months of special food! The preliminary encouragement from the illiterate criminals was intended to entangle the gullible victims into a strong emotional connection with the virtual pets so that they would be more willing to send a payment to the scammers.

So in sum, here are some principles we should have applied from the start before getting any further involved in this scam:

- 1. Before looking into the purchase (or adoption) or anything, immediately use a search engine to scan for identical unusual words, misspellings, or phrases. Look for multiple ads that have identical wording and photographs of the product or animal.
- 2. If there are photos of the product or creature, check Google Images to see if you can locate identical photos that suggest that the user is simply faking a picture.
- 3. If there is a phone number available in the ad, search for it using a search engine; be sceptical if there are multiple, mutually-exclusive hits. If someone claims to be in Northumbria and in Suffolk at the same time, something's wrong.
- 4. Be sceptical of offers that are too good to be true. Why would someone be giving away expensive products or animals to complete strangers?
- 5. Never agree to send money in advance of the delivery. There are ways of putting money in escrow (e.g., eBay's Buyer Protection for payments made through PayPal<
  <a href="http://pages.ebay.com/coverage/index.html">http://pages.ebay.com/coverage/index.html</a> >) so that neither buyer nor seller can be cheated.

We're still looking for a cat, but we're going to the local animal shelter this time.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:mekabay@gmail.com">http://www.mekabay.com/</a> >

\* \* \*

### **CLOCKWISE**

#### by John Laskey & M. E. Kabay, PhD, CISSP-ISSMP

Another welcome contribution from collaborator John Laskey. This is entirely John's work with minor editorial changes by Mich.

\* \* \*

Have you ever come across a profession that is the opposite of every element taught in information management and security?

I just did. For family reasons, I attended a conference of clock- and watchmakers. Themes included precision and accuracy and the attendees were all serious-minded professionals. Having much the same profile, in fact, as security professionals.

How, then, could this gathering be the antithesis of our profession? I'll highlight the differences, because sometimes it's just fun to compare outlooks from professionals whom you could expect to have much in common.

#### **Complexity**

This is a no-no from an information planning and security perspective. Remember Bruce Schneier's aphorism, "...[C]omplexity is the worst enemy of security"<
<a href="http://www.schneier.com/crypto-gram-0003.html">http://www.schneier.com/crypto-gram-0003.html</a> >? Our clock-makers, however, see complexity as absolutely a merit — I was startled early on in the conference by a PowerPoint slide that assessed the complexity of a prototype clock as one of five driving factors behind its design! Not only did this clock feature moving parts fashioned as little animals: the creatures were designed to move in ways that actually increased accuracy, while some of the cogs and wheels were designed so they would move in ways that would draw in the viewer's attention. So instead of concentrating on the end 'product' (i.e., telling the time) the observer is invited to appreciate and enjoy the spectacle of how the 'product' came about.

#### **Openness**

There is much debate about openness in security: from reporting vulnerabilities to the secrecy around some security architectures, particularly government ones. All of this is based on an argument that obscurity makes the job of potential attackers more difficult, despite the insistence of educators on Kerkhoffs' Principle<

http://www.mekabay.com/nwss/833\_lesson\_in\_a\_haystack--kerckhoffs\_principle.pdf >. By refreshing contrast, our clockmakers have a completely different perspective of the workings of their new designs. For one particularly complex clock, the presenter gave his audience a complete visual breakdown of how all of the working parts were made and how they would work together. This rather bracing outlook (from the perspective of a security professional and, perhaps, a patent lawyer) probably owed much to the fact that this clock was conceived in 1993, and was not due for completion until 2015. The design and the work put into the project were so complex and time-consuming that plagiarism was unlikely to be a problem. Incidentally I did not see or hear the word 'patent' at any point during the conference.

#### **Retrofitting and Add-Ons**

One feature of an IT architect's art is to reduce as far as possible the need for retrofitting, for instance by helping to identify and manage obsolescence in a new IT system and integrating security considerations from the start of the design. But the maker of the complex clock had thought up some pretty fundamental new ideas for its appearance since its original concept, and was adapting them into the design. A prototype of the clock looked a lot different than its drawing board concept, and the audience was invited to applaud the development of the clockmaker's ideas – even though they continued well beyond the implementation stage.

#### **Turnaround Times**

A major challenge for security developers is to keep in step with the system designers and the delivery timescales set by the system's owners and beneficiaries. As I have said, out clockmaker thought nothing of working on a design so complex that it would take 23 years from design to full implementation. And, he added, no computer-assisted measures had been used in the design: everything was done by hand, including the long calculations needed to ensure all the moving parts worked.

#### **Obsolescence**

IT designers, and security experts are often challenged by the question of obsolescence; a component might cease to be manufactured, or it might be too difficult to service, or be superseded by a better, cheaper, more secure method/component. Our clockmakers however think nothing of designing new, complex mechanical solutions to problems that you might consider already long solved. Some of us may, for instance, wonder why they seek new solutions in gears and wheels at all when there are plenty of electronic answers that are more precise and less prone to wear.

The answer is aesthetics. There are still many who appreciate mechanical timepieces (for some people, it is still a signature of success to show off a mechanical watch, if not necessarily a timepiece that takes 23 years to deliver). But I wonder: might a clock-maker be very good at systems design and security? Or might a professional security person be able to design and deliver a mechanical timepiece?

\* \* \*

John G. Laskey< <a href="http://www.linkedin.com/pub/john-laskey/28/b28/b69">http://www.linkedin.com/pub/john-laskey/28/b28/b69</a> is a US-based security consultant who has worked for the UK government equivalents of DHS and FEMA. As IT Security Officer for the Home Office he was responsible for the security risk management of a number of high profile systems developed to increase government and public security. Recently, John helped launch the CESG Certified Professional scheme for IA consultants seeking UK government contracts. John has advised senior UK government managers on the health of major projects and programs and he is a certified lead auditor for the ISO 27001 security standard. He is a member of BCS – the Chartered Institute for IT – and of the Institute of Information Security Professionals (IISP).

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:mekabay@gmail.com">http://www.mekabay.com/</a> >

Copyright © 2012 John Laskey & M. E. Kabay. All rights reserved.

## **Don't Participate in Porn2Porn Networks**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

A colleague recently told me that a young relative of his was arrested by the state police in his US home for obtaining and distributing child pornography.

Child pornography is defined as "any visual depiction of sexually explicit conduct involving a minor (persons under 18 years of age).... Federal law prohibits the production, distribution, importation, reception, or possession of any image of child pornography."<a href="http://www.justice.gov/criminal/ceos/subjectareas/childporn.html">http://www.justice.gov/criminal/ceos/subjectareas/childporn.html</a>

In a 2001 paper< <a href="http://www.cyber-rights.org/documents/us\_article.pdf">http://www.cyber-rights.org/documents/us\_article.pdf</a> >, "Governing Pornography & Child Pornography on the Internet: The UK Approach" (in *Cyber-Rights*, *Protection, and Markets: A Symposium. University of West Los Angeles Law Review* 247:275) from Yaman Akdeniz, LLB, MA, PhD, then of the CyberLaw Research Unit of the Faculty of Law at University of Leeds< <a href="http://www.law.leeds.ac.uk/research/international-governance/cyberlaw-research-unit/">http://www.law.leeds.ac.uk/research/international-governance/cyberlaw-research-unit/</a> > (and also the Founder and Director of the Cyber-Rights & Cyber-Liberties organization</a> <a href="http://www.cyber-rights.org/">http://www.cyber-rights.org/</a> >), Dr Akdeniz points to two UK laws particularly concerned with prosecuting child pornography (including "pseudo-photographs", which are modified images made to appear to be child pornography):

- Protection of Children Act of 1978
- §160 of the Criminal Justice Act of 1988.

As in the USA, creation, possession, and distribution of such materials are all punishable by law in the UK.

The young man who was arrested protested his innocence; apparently the illegal images were found only in the folders associated with a peer-to-peer (P2P) network that he belongs to. P2P networks such as the early versions of Napster< <a href="http://www.napster.com/">http://www.napster.com/</a> > and Kazaa<<a href="http://www.crunchbase.com/company/kazaa">http://www.crunchbase.com/company/kazaa</a> > allow (or allowed) users to post files for easy sharing with any other member of the network. Some of the shared files distributed through P2P networks that have been studied intensively are illegal copies of music, videos and software.</a> <a href="http://law.vanderbilt.edu/publications/journal-entertainment-technology-law/archive/download.aspx?id=3190">http://law.vanderbilt.edu/publications/journal-entertainment-technology-law/archive/download.aspx?id=3190</a>>

A current example of a server-based equivalent to these P2P networks is Dropbox<a href="https://www.dropbox.com/tour">https://www.dropbox.com/tour</a>, which lets a group of people access shared files instantly.

Another quirk is that some inoffensive-looking programs include file-transfer capabilities that most users fail to notice. For example, digsby < <a href="http://www.digsby.com/">http://www.digsby.com/</a>> is a multiprotocol instant messenger client that integrates e-mail services and social-networking services into a single user interface. However, the terms of service< <a href="http://www.digsby.com/tos.php">http://www.digsby.com/tos.php</a> > changed after 2008.12.16 and before 2009.02.26<

http://web.archive.org/web/20090226041618/http://www.digsby.com/tos.php > (ascertained using the Wayback Machine) to state that

"You agree to permit the Software to use the processing power of your computer when it is idle to run downloaded algorithms (mathematical equations) and code within a process. You understand that when the Software uses your computer, it likewise uses your CPU, bandwidth, and electrical power. The Software will use your computer to solve distributed computing problems, such as but not limited to, accelerating medical research projects, analyzing the stock market, searching the web, and finding the largest known prime number. This functionality is completely optional and you may disable it at any time."

When I used Digsby several years ago, I failed to read clause 15 in the Terms of Service and therefore had no idea that the program was silently using my resources for anything at all other than my commands. When I found out, I uninstalled the program in a fit of pique.

The problem for users of any networks that download files to their computers without necessarily providing information about what is being transferred via the users' computers is that the users don't have information about what is being transferred via their computers!

Aside from the risk of malware infection< <a href="http://threatpost.com/en\_us/blogs/hidden-security-risks-p2p-traffic-062712">http://threatpost.com/en\_us/blogs/hidden-security-risks-p2p-traffic-062712</a> >, P2P programs pose serious legal risks for users and for the corporate owners of the equipment being used to support P2P traffic. Joe Dysart write in *Today's Campus*<a href="http://www.todayscampus.com/articles/load.aspx?art=369">http://www.todayscampus.com/articles/load.aspx?art=369</a> > that

"Many P2P users are being less-than-careful about the folders that get shared when they install a P2P program and are unwittingly disseminating all sorts of personal, sensitive and potentially damaging data over the web.

"The Committee staff did its own investigation," says U.S. House Rep. Henry Waxman, who chairs the House's Committee on Oversight and Government Reform. "We used the most popular P2P program, LimeWire, and ran a series of basic searches. What we found was astonishing: personal bank records and tax forms, attorney-client communications, the corporate strategies of Fortune 500 companies, confidential corporate accounting documents, internal documents from political campaigns, government emergency response plans and even military operation orders."

Worst case scenario for a university: a staff member using P2P software could inadvertently download a child porn image coded with a clandestine file name and never know it until it was too late, says Pasquale Giordano, president and COO of SafeMedia, a company that specializes in P2P blocking technology.

Readers would do well to either avoid P2P technology or to monitor the contents of files being transferred through these networks to ensure that they are not inadvertently contributing to crimes and inadvertently ending up being arrested.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:mekabay@gmail.com">http://www.mekabay.com/</a> >

### **Cyberethics and Civil Discourse**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

In one of the many interesting presentations at the annual Securing the eCampus conference <a href="http://www.ists.dartmouth.edu/events/ecampus/">http://www.ists.dartmouth.edu/events/ecampus/</a> > organized by the the Institute for Security, Technology, and Society (ISTS) <a href="http://www.ists.dartmouth.edu/about/">http://www.ists.dartmouth.edu/about/</a> > at Dartmouth College in July 2012, Edward Pittman, EdD<a href="http://www.ists.dartmouth.edu/about/">http://www.ists.dartmouth.edu/about/</a> > at Dartmouth College in July 2012, Edward Pittman, EdD<a href="http://www.ists.dartmouth.edu/about/">http://www.ists.dartmouth.edu/about/</a> > at Dartmouth College in July 2012, Edward Pittman, EdD<a href="http://www.vassar.edu/">http://www.ists.dartmouth.edu/about/</a> > at Dartmouth College in July 2012, Edward Pittman, Edward Pittman, EdD<a href="http://www.vassar.edu/">http://www.vassar.edu/</a> > at Vassar College <a href="http://www.vassar.edu/">http://www.vassar.edu/</a> > discussed "Cyberethics, Discourse and Campus Community." <a href="http://www.vassar.edu/">Dr Pittman's career includes 28 years of experience in university affairs, including diversity education. Some of his work concerned consequences of increasing diversity on campus. Comments in [square brackets] are MK's alone.

Dr Pittman presented a fascinating overview and case study of how one college has tried to encourage environments for civil discourse in cyber world; he sparked discussion about opportunities and challenges for higher education in this arena. He defined *cyberethics* as a code of behavior that governs the Internet and other forms of electronic communication in the cyberworld. One form of defining moral or ethical behavior is to see if a proposed course of action would be doing more good than harm; however, the Internet is usually viewed as supporting generally positive results (e.g., getting information quickly [unless you are a Chinese or Syrian dictator]).

College students can see and contribute to a wide range of sites on the Web to post their opinions; e.g., b@b< http://boredat.com/ >, Facebook postings, MadsVassar blog< http://www.madsvassarblog.com/ >, RateMyProfessor< http://blog.ratemyprofessors.com/ >, and Collegiate ACB (Anonymous Communication Board)< http://collegiateacb.com/ >. "Gossip servers" have become a source of distress for many students: there is no way of identifying the source of scurrilous and offensive comments. [For an extensive collection of chapters discussing many aspects of social media, see Noor Al-Deen, H. S. & J. A. Hendricks (eds). *Social Media: Usage and Impact.* Lexington Books (ISBN 978-0-7391-6729-8 paper or 978-0-7391-6730-4 electronic). AMAZON < http://www.amazon.com/Social-Media-Usage-Impact-ebook/dp/B0062ZQZBA >. In particular, Chapter Fourteen, "Legal Pitfalls of Social Media Usage" by L. B. Lidsky & D. C. Friedel discusses legal redress for online defamation and harassment.]

The proliferation of Websites and social-networking sites that can be used to support political activity has generated debate on college campuses. [For example, the *Campaign to Stop Killer* Coke < <a href="http://killercoke.org/downloads/kccvassar.pdf">http://killercoke.org/downloads/kccvassar.pdf</a> > has spawned many college clubs such as those at Vassar < <a href="http://killercoke.org/downloads/kccvassar.pdf">http://killercoke.org/downloads/kccvassar.pdf</a> >, Swarthmore's group < <a href="http://www.swarthmore.edu/news-and-events/news-archive-2006-2007/swarthmore-removes-coca-cola-products-from-campus.xml">http://www.archive-2006-2007/swarthmore-removes-coca-cola-products-from-campus.xml</a> >, University of Vermont <a href="http://www.7dvt.com/2006/students-campaign-kick-coke-campus">http://www.7dvt.com/2006/students-campaign-kick-coke-campus</a> >, New York University <a href="http://socialistworker.org/2010/05/03/nyu-campaign-against-coke">http://socialistworker.org/2010/05/03/nyu-campaign-against-coke</a> >, and University of Michigan <a href="http://www.organicconsumers.org/school/mi.cfm">http://socialistworker.org/2010/05/03/nyu-campaign-against-coke</a> >, and University of Michigan <a href="http://www.organicconsumers.org/school/mi.cfm">http://www.organicconsumers.org/school/mi.cfm</a> > among others. Naturally, these campaigns have led to vigorous debate <a href="http://www.madsvassarblog.com/2008/10/sound-off-should-we-kick-coke.html">http://www.madsvassarblog.com/2008/10/sound-off-should-we-kick-coke.html</a> > that has sometimes led to escalation of hostility through electronic communications. For example, anonymous commentators in the *Mads Vassar Blog* cited here wrote,

- "i wish these kids would STFU."
- "Before 7:01[posting-time is being used as an identifier for the anonymous post], this comments page reads like an Asshats For Palin forum. Shame on you apathetic, self-important douchebags."

• "Open your eyes. Read a book. You fucking privileged, entitled children, you don't even realize or give a damn what other people spend their lives suffering through and fighting against, and what kind of a CHOICE do you think they have?"]

In another case, the Vassar student publication *The Imperialist* published unedited commentary in 2005 that offended many students on campus. In the interval of the interval of the article challenged the very concept of diversity programs on college campuses and included disparaging comments about various communities. Student activists were offended, and non-campus people and Websites were able to repost the conversations from the campus community. Nazi and other racist groups published excerpts and included threats and defamation; however, it was not possible to force takedown of these materials or to suppress such speech in *The Imperialist*.

The students and administration at Vassar responded to the fundamental question of how to cope with these issues. Although campus regulations on harassment can be applied to behavior using computers and the computer regulations section in the *Student Handbook* forbid the use of College computers for criminal activities or business, few students were thought to be reading those regulations.

The *Student Handbook* was updated and a Committee on College Life< <a href="http://committees.vassar.edu/">http://committees.vassar.edu/</a> >set up by the Governors of the College and including five elected faculty members, seven student representatives as functions of their position in student government, and administrators related to student life. They formed a subcommittee to supplement computer regulations to educate students and issued a statement adopted the Spring 2012 semester that included this major prohibition: "Behaviors that create harmful effects include illegal activities, offensive and defaming language, hate speech, postings of private information such as phone numbers and addresses, posting private photos, and anonymous messages that target individual or groups."

Dr Pittman ended his talk with questions for higher education:

- What is our responsibility toward creating environments for civil discourse?
- Where is the line between free speech or expression and self- and community responsibility?

[I think that all of us need to think about these questions and to provoke constructive discussions in our institutions and in society at large.]

My thanks to Dr Pittman for an animated and thought-provoking presentation.

\* \* \*

M. E. Kabay, < <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials. <a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

## **Operational Essentials**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

We have a terrific student chapter< <a href="http://www.acm.org/chapters/students">http://www.acm.org/chapters/students</a> > of the Association for Computing Machinery(ACM)</a> <a href="http://www.norwich.edu">http://www.norwich.edu</a> >. The School of Business and Management</a> <a href="http://programs.norwich.edu/business/">http://programs.norwich.edu/business/</a> > provides the students with a clubroom that is next to the academic computer lab and to the rooms reserved for the Cyber Weapons Range War Room</a> <a href="http://www.7dvt.com/2010norwich-university-advanced-computing-center">http://www.7dvt.com/2010norwich-university-advanced-computing-center</a> >.

The academic lab is for classes requiring access to specific software (e.g., statistical packages) and supporting access to the University's electronic classrooms where many of us post links to resources, assignments, quizzes, and facilities for uploading and grading assignments. Examples drawn from this semester's schedule include classes in Chinese language, construction engineering management, basic computer skills, introduction to business, college algebra, nursing informatics, construction project management, differential equations, experimental psychology, and applied statistics.

The War Room is used for specialized courses and events such as network attack/defend exercises and contests, system administrator training, live demonstrations for security conferences (using telepresence), digital forensics analysis and cyber criminalistics. The War Room has state-of-the-art wall-mounted large-screen displays, top-quality digital video cameras for interactive presentations, two dozen workstations and access to high-speed intranet and Internet connections. Much of the work is done through virtualized systems running on rack-mounted servers described in the article referenced earlier< <a href="http://www.7dvt.com/2010norwich-university-advanced-computing-center">http://www.7dvt.com/2010norwich-university-advanced-computing-center</a>>.

Recently I had a meeting with computer club members who currently run the servers we depend on for the War Room and for many of our online courses. These are some of our brightest kids; they're fascinated by a wide range of knowledge, eager to pursue answers to interesting questions, friendly to each other and to less gifted students, and committed to supporting the progress of our computer science, information assurance, and cyber-forensics programs.

The team of six students and I spent 90 minutes late on a Friday afternoon brainstorming about how to convert a student club oriented towards learning – and fun – into an operationally sound team that can guarantee quality of service defined in service-level agreements – and maintain the fun.

We started off with some brainstorming to identify what has to be done to maintain and further the services and to list specific problems facing the group. Within a few minutes, we'd identified and classified the following points as key issues:

- Operations (keeping the hardware and operating environment running
  - We have commitments to paying customers such as the College of Graduate and Continuing Studies who depend on the online courses we make available.
  - o Although we haven't formalized our quality of service (QoS) into service-level agreements (SLAs), we still face implicit expectations among our users about

availability and response time.

- Production (meeting the requirements for specific projects)
  - We are constantly given new requirements as the reputation of the service expands.
  - We have to formalize the procedures for scheduling and building the resources for specific tasks.

#### • Business Continuity Planning

- We have too many single points of failure, including individuals we count on who are the only ones with specific critical knowledge.
- We have a big uninterruptable power supply that can handle critical servers and an external electrical generator; neither has been installed because we don't have the budget yet to move them over to our installation.
- We need to plan and effect regular off-hours and then live testing of our capabilities.
- Our network infrastructure is vulnerable; we have only two Internet Service Providers (ISPs) and both are local services. A major wind- or ice-storm such as Tropical Storm Sandy
  <a href="http://alerts.weather.gov/cap/wwacapget.php?x=VT124CCABB19AC.HighWind-Warning.124CCABD2D50VT.BTVNPWBTV.0a502f8f5bf8e0d07e392425a6f0e-1d4">http://alerts.weather.gov/cap/wwacapget.php?x=VT124CCABB19AC.HighWind-Warning.124CCABD2D50VT.BTVNPWBTV.0a502f8f5bf8e0d07e392425a6f0e-1d4</a> > could disrupt services to remote and local users.
- Much of our operational infrastructure is either completely undocumented or is documented only on scraps of paper that are impossible to search quickly or to backup effectively.
- We need to re-evaluate our backup policy, including off-site storage.

#### • Disaster Recovery Planning

o If the systems must be replaced due to major disruptions such as physical damage and extended failure of our network infrastructure, how will we resume operations?

#### • Personnel Management

- We don't have a formal recruitment program to encourage younger students to join the group and develop their technical skills.
- We have no one who monitors all contact information for every member of the team.
- We're still using e-mail for communications instead of a permanent user group where our messages and documentation files are archived for future team members to be able to access.

So what lessons can readers derive from this situation?

- Enthusiastic amateurs are a great resource for testing out ideas and building prototypes but they cannot substitute for thorough, meticulous planning once we move to a production environment.
- The natural aversion to documentation cannot be permitted to interfere with development
  of a corporate knowledge base that will allow future members to come up to speed
  quickly.
- Policies and procedures are necessary for a production environment to survive.
- Someone has to be in charge of personnel management: the future of a student organization depends on a steady supply of fresh enthusiasts who can be trained quickly.
- Business continuity planning and disaster recovery may be minor issues during the prototyping phase, but as systems move into production, they become essential.

As you can imagine, the students left with an extensive TO DO list. We'll keep meeting every

week and I'll occasionally report on our progress.

In the meantime, here are some resources about operations and system management that readers may find helpful.

- Documentation for Less Work: Will this Have to be Done Again?< http://www.mekabay.com/opsmgmt/documentation.pdf >
- Facilities Management in the Age of Information Warfare
   <a href="http://www.mekabay.com/opsmgmt/facmgmt.pdf">http://www.mekabay.com/opsmgmt/facmgmt.pdf</a>
- Review of Visible Ops Security< <a href="http://www.mekabay.com/opsmgmt/vos.pdf">http://www.mekabay.com/opsmgmt/vos.pdf</a>
- Staffing the Data Center < <a href="http://www.mekabay.com/opsmgmt/staffing.pdf">http://www.mekabay.com/opsmgmt/staffing.pdf</a> >
- System Logging < http://www.mekabay.com/opsmgmt/logging.pdf >
- Computer Security Incident Response Team Management
   http://www.mekabay.com/infosecmgmt/csirtm.pdf >
- Facilities Security Audit Checklist< http://www.mekabay.com/infosecmgmt/facilities\_checklist.pdf >
- Preparing for the Next Solar Max< <a href="http://www.mekabay.com/infosecmgmt/solarmax.pdf">http://www.mekabay.com/infosecmgmt/solarmax.pdf</a>

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:mekabay@gmail.com">http://www.mekabay.com/</a> >

\* \* \*

## **Brainstorming SOPs**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

The developments at the Norwich University Center for Advanced Computing<
<a href="http://www.nuacc.org/">http://www.nuacc.org/</a> continue. A few days before this article went to press, Vermont was alerted to the major risks of heavy rain and wind from Hurricane Sandy<
<a href="http://www.boston.com/news/weather/2012/10/29/superstorm-glance-vermont/8ndUqwdBJBnmAWQMEKzHiJ/story.html">http://www.boston.com/news/weather/2012/10/29/superstorm-glance-vermont/8ndUqwdBJBnmAWQMEKzHiJ/story.html</a> and the strong possibilities of major electric power outages. Our emergency generator and large-scale uninterruptable power supply have arrived at the University but are not yet installed, so our director, Peter R. Stephenson, PhD, CISSP, CISM, FICAF, LPI, made the decision to bring the systems down on Monday afternoon to prevent catastrophic damage to our virtual systems – crashing virtual pods can result in days of work to re-establish clean virtual machines. We announced that the systems would not be available to support the electronic classrooms that are used for distance-education courses managed by our College of Graduate and Continuing Studies</a> <a href="http://graduate.norwich.edu/">http://graduate.norwich.edu/</a>>.

We've been working on formalizing our operations documentation, so a group of us including senior student Jacob Berry as our scribe, met to brainstorm about the structure of standard operating procedures (SOPs). What follows is my interpretation of our discussions; I hope that the ideas will be useful to others and that we can stimulate discussion and information sharing that can help us all improve our SOPs.

The first issue for all SOPs is that we need a unique name, including a sequence number that immediately helps put the SOP in the right context. For example, if our procedures have six sections, and continuing operations are in section 4, then all the operations procedures will be numbered as 4.n (4.1, 4.2, etc.).

Each SOP should include a statement of its purpose. Why do we need this procedure? What does it enable us to do that we can't do without it? This approach is based on the operations credo that every SOP must materially affect our operations.

We need to define the scope of our SOP. What systems and components are involved? For example, which hardware? Which software? Which networks? Which services (such as courses)? Which customers (or groups of customers) are affected (e.g., students in a specific college of the University?

Who are the responsible staff members affected by this SOP? These identities must be role-based and name titles, not personal names. Three classes of people affected by a SOP are

- Those who *authorize* action according to the SOP;
- People who *act* on the SOP;
- People who should be *informed* (e.g., clients, suppliers...) as part of the SOP.

A useful component of any SOP is the critical-path analysis <a href="http://www.mindtools.com/critpath.html">http://www.mindtools.com/critpath.html</a> which shows where a procedure fits in the larger schema of operations (e.g., "this SOP is part of the business-continuity section"). What must be done before we can engage this procedure? What sequence of steps (processes) must be followed

to complete the SOP? Which processes can run in parallel within the SOP? What are the possible next steps we might undertake after we complete this SOP?

The SOP must detail all the processes, with explicit numbering to allow everyone in the team to refer to the same process without ambiguity. The processes all have to stipulate what we have to do and how we tell if our process has completed successfully. In addition, we must define how to respond if a process did not work as planned.

OK, so that was a good start.

We continued our discussion with some notes on possible status levels that could be useful in our operations. The primary goal of defining a set of status levels is to improve communications among the operations staff and with customers. Each status level must define how to decide to change from one level to another. The metrics for our Center include the likelihood of degraded quality of service (QoS) or the actual degraded QoS. We settled on a preliminary sketch of four levels and our notes are reasonably clear:

- Green (Normal administration team)
  - No likelihood of degraded QoS
  - Systems are fully operational
- Yellow
  - Low likelihood of degraded QoS
  - Heightened alert to monitor situations
  - No other actions required
  - o Who's involved: Normal administration team
- Orange
  - High/Medium likelihood of degraded QoS
  - o Growing risk of failure
  - o Performing actions to prepare for failure
  - QoS not yet degraded
  - Who's involved: Computer Emergency Response Team (CERT) monitoring and planning to assure business continuity or to safeguard equipment
- Red
  - QoS is degraded
  - o Systems are at high levels of failure
  - Operational issues
  - Systems off
  - Whole class room fails
  - Who's involved: CERT actively responding to situation to safeguard equipment and assure speedy restoration of QoS.

Another short discussion concerned defining several out-of-band communications tailored to client preferences. Because we may experience downtime, we choose to use communications that don't depend on continued operations of the Center. Ideas include e-mail, short-message service (SMS) text alerts to mobile devices, a Webpage (possibly using Facebook), and Twitter. Clients would choose any or all of these channels as they see fit.

Finally, we tentatively resolved on a summary definition of who should be in our CERT: the Director, the Associate Director (me), all senior team members, and all lead administrators.

That's the status for now; I'll keep you posted on anything interesting that comes up as we progress.

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

### Winn Schwartau's Excellent Adventure

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Winn Schwartau< <a href="http://www.allamericanspeakers.com/celebritytalentbios/Winn-Schwartau">http://www.allamericanspeakers.com/celebritytalentbios/Winn-Schwartau</a> has been an inspiration to me for over twenty years. The man is brilliant, tireless, articulate, productive, innovative, and kind. We met through the National Computer Security Association in the early 1990s and he influenced me enormously with his book *Information Warfare*, now available in its Second Edition as a Kindle e-book.<a href="http://www.amazon.com/Information-Warfare-ebook/dp/B00428LB4U">http://www.amazon.com/Information-Warfare-ebook/dp/B00428LB4U</a> > When I organized the First International Conference on Information Warfare in 1993, he was our keynote speaker. He remains a dear friend to this day.

Winn has founded so many successful organizations that his LinkedIn profile<
<a href="http://www.linkedin.com/in/winnschwartau">http://www.linkedin.com/in/winnschwartau</a> > looks like several people's careers have been crammed together. The man simply won't stop!

To my knowledge, Winn was the first security expert explicitly to refer to a "digital Pearl Harbor," sometime in the early 1990s – a term that has caused considerable controversy in recent times (just look up the phrase in quotation marks in a search engine).

Searching for "Schwartau" in *NetworkWorld's* published materials< <a href="http://www.networkworld.com/search/index.html?cx=014839440456418836424%3Amzedprvnwmy&cof=FORID%3A9&ie=UTF-8&q=schwartau&x=0&y=0">http://www.networkworld.com/search/index.html?cx=014839440456418836424%3Amzedprvnwmy&cof=FORID%3A9&ie=UTF-8&q=schwartau&x=0&y=0</a> > brings up over half a million hits. His writing is challenging and incisive and his articles are fun to read even decades after he published them.

In 1991, he published the novel *Terminal Compromise*, < <a href="http://www.amazon.com/Terminal-Compromise-Computer-Terrorism-Networked/dp/0962870005/">http://www.amazon.com/Terminal-Compromise-Computer-Terrorism-Networked/dp/0962870005/</a> > which still ranks as one of my all-time favourite science-fiction novels.

Another excellent book of his is the 2001 *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption.*<a href="http://www.amazon.com/Cybershock-Surviving-Phreakers-Terrorists-Disruption/dp/156025307X">http://www.amazon.com/Cybershock-Surviving-Phreakers-Terrorists-Disruption/dp/156025307X</a> > He reviewed the criminal-hacker culture, cyber-scams, denial of service, cyber-defence methods, and possible future developments.

One of the themes that he has pursued with enthusiasm and commitment is providing educational materials for children and parents about safe use of computers and networks ("cybersafety"). Building on his extensive experience as an industry security evangelist<
<a href="http://www.thesecurityawarenesscompany.com/about/winn.html">http://www.thesecurityawarenesscompany.com/about/winn.html</a> >, he wrote *Internet & Computer Ethics for Kids:* (and Parents & Teachers Who Haven't Got a Clue)<
<a href="http://www.amazon.com/Internet-Computer-Ethics-Kids-Teachers/dp/0962870056">http://www.amazon.com/Internet-Computer-Ethics-Kids-Teachers/dp/0962870056</a> > in 2001.

Now he wants to update it.

Winn and his family (the kids are incredibly talented) are planning updates to maintain the tone of the first edition:

"Cyber Safety and Ethics and Stuff is an easy to read, colorful and visually appealing book, written for the entire family and K-12 schools. The goal is for families to talk; for teachers to use these ideas in classrooms and discuss the important safety, privacy and security challenges everyone from 8 to 80 faces online today."

#### Key topics include

- Hacking,
- Internet Scams
- Facebook Privacy
- Cyber Bullying
- Plagiarism
- PC Security Basics for Home
- iPhone, iPad and Mobile safety
- Phishing attacks
- Adult materials
- Stealing
- Personal online responsibility

Using the crowd-sourcing tool *Kickstarter*,<

http://www.kickstarter.com/projects/winnschwartau/cyber-safety-and-ethics-and-stuff > he is appealing for funds to make sure that 50,000 to 1,000,000 free copies can be distributed to schools and the children, teachers and parents who can benefit from the up-to-date information and non-moralistic tone of the work. I just donated a modest amount and I hope that you will contribute!

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

## **Not So Cloudy Now**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

In recent years, increases in bandwidth for Internet connectivity have opened practical options for online backup.

Alan Freedman's *Computer Desktop Encyclopedia*< <a href="http://computerlanguage.com/">http://computerlanguage.com/</a> > defines "cloud storage" as follows:

#### "cloud storage

Storing or backing up data over the Internet. There are numerous third-party storage providers that let users upload and store any type of computer file. Also called "online storage" or "public cloud storage," the files can typically be shared with or without passwords to someone with Internet access and a Web browser. Many services offer a limited amount of disk space for free with monthly fees for higher capacities. Some providers offer storage for a monthly fee per gigabyte.

#### **Cloud Sync**

Cloud storage providers often feature synchronization, which ensures the same set of files are updated on all the user's devices. In such cases, a client program may need to be installed in the user's device to employ this capability.

#### **Large Files and Executables**

Cloud storage is also used to transfer large files to another user rather than via e-mail attachments, which are often rejected by the mail system due to file size limitations. In addition, mail servers often refuse attachments that are executable files, whereas cloud storage typically has fewer restrictions. See e-mail attachment.

#### **Cyberlockers and Content Management/Delivery**

Services that provide cloud storage for the express purpose of sharing media with the public are often called "cyberlockers." Cloud storage providers that hold data to be sent to a user's application or Web browser on demand fall under the "content management" umbrella (see CDN). See *cloud storage gateway*, *S3 cloud storage*, *external storage* and *media sharing site*."

One cloud-storage vendor, **BACKBLAZE**< <a href="http://www.backblaze.com/">http://www.backblaze.com/</a>>, summarizes the added value of online backups even for PC and Mac users who have external hard drives for their backups:

"It's a good start, but as our vice president of design says, "better safe than sorta safe." Do you back up your data every day? Or do you sometimes forget? Are you sure you're backing up the right files? Are your computer and USB drive stored in the same place,

making both susceptible to the same risks? What if you go on a trip and leave the drive at home? You can't backup or restore files while you're gone. And if you take it with you? Then you're more likely to lose both your laptop and USB drive at the same time!"

David Robbins (*NetworkWorld* <

http://www.pcworld.com/article/164933/cloud\_computing.html >) points out that cloud computing has fundamental benefits and limitations for all types of information technology (IT) applications:

"Cloud services typically have the following characteristics:

- They can be rapidly deployed, so they are quick to value.
- There is little or no start-up cost and no capital investment.
- Costs for services are usage based with no fixed commitment.
- Services can be quickly and easily scaled up or down with no penalty.
- Services are multi-tenant (many customers leverage the platform).
- The ability to customize a service is limited."

#### He adds,

"As with any service, with the cloud you should always make sure that you know what you are paying for and what measurements exist to show you are actually receiving the service. You should pay careful attention to:

- Service levels Cloud providers may be hesitant to commit to consistency of performance for an application or transaction. Understand the service levels you can expect for transaction response times, data protection and speed of data recovery.
- Privacy Someone else hosting and serving your data could be approached by the U.S. government to access and search that data without your knowledge or approval. Current indications are that they would be obligated to comply.
- Compliance You are probably already aware of the regulations that apply to your business. In theory, cloud service providers can meet the same level of compliance for data stored in the cloud but, because most of these services are young, you'll need to take extra care.
- Data ownership Do you still own your data once it goes into the cloud? You may
  think the answer to this question is obvious, but the recent flap over Facebook's
  attempt to change its terms of use suggests that the question is worth a second
  look.
- Data Mobility Can you share data between cloud services? If you terminate a cloud relationship can you get your data back? What format will it be in? How can you be sure all other copies are destroyed?"

Keith Thomas, writing in *PCWorld*,<

http://www.pcworld.com/article/223354/choosing\_cloud\_backup\_for\_pcs.html > summarizes the issues in choosing cloud backup services as follows:

- Dedicated backup services monitor designated files and create time-stamped backups when the targets change.
- Cloud synchronization services copy the contents of selected folders or disk drives to an equivalent online.
- Some services allow for delta backups: storing changes in target files instead of clogging connections with entire large files when a few records are changed.

- Defining the time and priority for data transfer is essential; some services allow low-priority and off-peak data transfers so that backups don't interfere with workstation performance.
- Not all consumer-oriented services include recovery functions; backup may be easy, but in these cases, restoring the data may be complex and time-consuming.
- Such services typically provide encryption for the stored contents, including options for encrypting the data before transfer instead of allowing the service to perform the encryption.
- Proprietary encryption may lock a user into using a particular service and if different clients (PC, Mac, UNIX) don't have access to the appropriate client software, a disaster on one platform may preclude restoring data to a different computer.
- The stability of the cloud-backup service is an issue; if a company fails to back up its clients' data, many users may be affected.

A review site, **top-10-online-backups.com**< <a href="http://www.top-10-online-backups.com/best-cloud-storage?per\_page=100&storage\_space=&price=&file\_sharing=">http://www.top-10-online-backups.com/best-cloud-storage?per\_page=100&storage\_space=&price=&file\_sharing=</a> > lists 30 online backups and provides reviews brief reviews of each product; unfortunately, some of these "reviews" are by (mostly disgruntled) anonymous users.

Potential users will want to research specific candidates with up-to-date, professional reviews.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:mekabay@gmail.com">http://www.mekabay.com/</a> >

\* \* \*

## Walk What You Talk: Upper Management Must Support INFOSEC

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

The original version of this article was published in **Secure Computing Magazine** in 1995. The file is no longer available online, so we're republishing it here with minor updates.

The VP of Finance was in a hurry. He did stop his headlong rush towards his office long enough to get a temporary security badge from the guard station, but then he just ran through the gate without using the card to trip the card reader. As he ran down the hall, the guard shrugged and reset the alarm. "Well," shrugged the guard, "at least he asked for a badge. Most of the senior executives here wouldn't even bother with that."

This incident occurred during my security audit of a large corporation in the early 1990s. One of the problems of the corporate culture at this client site was that most people did not wear their photo-ID cards visibly; they concealed them under jackets or sweaters. During meetings with top executives, it became clear why this should be: the top of the corporate ladder was setting a terrible example. Despite protestations of commitment to security, they showed contempt for security. The top echelons:

- Did not wear their badges;
- Insisted on one-letter passwords;
- Gave their secretaries their e-mail IDs and passwords instead of arranging for proxy rights;
- Demanded complete access to restricted zones such as the server room despite having no reason to be present alone in these areas.

It is much worse for security when high-ranking staff flout policies and procedures than when lower-ranking staff do. The problem is that people come to associate lack of respect for security with high rank – and so they imitate the behaviour consciously or unconsciously.

Consider the experience of e-mail implementers in the early years. One outstanding principle was enshrined in everyone's handbook of how to succeed at e-mail: start from the top and work down. If your boss used e-mail, you would too, simply to keep in contact. On the other hand, if only clerks used e-mail and senior executives disdained it, then middle managers and everyone else would avoid the new system because they unconsciously wanted to look important. The same phenomenon accounts in part for the resistance by some executives to direct keyboard interactions with their e-mail systems in the old days: they associated typing with secretaries and they looked down on secretaries despite their intense dependence on their colleague's competence and efficiency.

At one site I evaluated, a senior administrator insisted on having master keys that could open every single lock in the entire building, including dust closets. This person had confused access with power. In a similar vein, directors who demand access codes for secured areas where they have no business are sending a dangerous message to everyone else: ignore need to know – knowledge is power. How then are we security managers to counter the demand from the

programming manager to have access to the server room? And how will the programming manager deny access to production data to the programming staff? And then whither separation of duties?

The tendency to imitate high-status individuals is deeply rooted in our biology and in our culture. Among other primates, individuals cluster around alpha males and females as if the leader's power will leak over to them. In human societies, we see cults of personality worldwide. We find millions of people admiring and imitating screen and music stars. Children and adolescents, especially, wear special clothes to fit into their group; when was the last time you saw a teenager wearing a cap with the bill on the front? Adults spend inordinate time, money and effort buying new clothes simply to be "in fashion." So why would anyone think that these habits stop at the door to the workplace?

The workplace is a community – sometimes the only community we know. Like all communities, it has a culture: what many call the corporate culture. Within the corporate culture, there are leaders, either by virtue of their position in the hierarchy or by virtue of their personalities. If the leaders wear purple socks for a week, the frequency of purple socks among the rest of the staff will gradually increase. If the executives play golf, the middle managers will take up golf. This may strike some as silly, but it is inevitable. Human beings are social creatures. We can override our tendency to imitate but it is always part of us. It is because of these deep impulses, rooted in evolution and culture, that we have to convince upper management that they are crucial links in the chain of defence of corporate data. Without their example, the edifice of trust will crumble.

In America, the aboriginal peoples have a saying: Walk what you talk. It's time for upper management to walk what they talk.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:mekabay@gmail.com">http://www.mekabay.com/</a> >

\* \* \*

# **Implants**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

"Daddy, why is there a Yinghui poster floating in front of the holovision display?"

Six-year-old Mei seemed puzzled but not alarmed.

"What do you mean, a poster?" asked her dad through his neural link, eyes opening wide in concern as he switched his receiver into high-volume mode.

"It says, 'U r .." she paused and spelled out the next word, "... p-w-n-e-d."

Xiayue Dien was an implant engineer at DienhuaKwai Corporation, makers of the real-time-access implants he and his daughter were using to watch the live HV feed from the lunar volleyball tournament. He accessed his daughter's sensory feed and the hair on his neck tickled as he felt the blood drain from his face.

"Um, sweetie, don't worry about it. The message is some sort of joke, I'm sure."

Actually, Dien was far more worried than he let on. The fact that the message was inserted at all was alarming enough, but having "English" inserted into an implant's output was terrifying. The criminal hacker gangs from Bei Mei had been trying to crack the dynamic encryption routines on the RTAs for years, but until recently, they'd never managed to penetrate the cyclic asymmetric algorithm that ensured that the data streams couldn't be corrupted.

"Pwned" was an ancient word dating from the late 20th century that meant roughly "owned" or "controlled." It had been popular until about a hundred years ago, in the mid-21st century but had died away – until last year, when reports surfaced on the internal networks that a few users of the latest three models of the RTA units were noticing intrusions into their data streams.

The first report he had seen referred to a relatively young woman of 62 in Fuzhou who experienced inexplicable movements of her prosthetic left hand; the first three fingers were waggling back and forth for 30 seconds at what seemed at first to be random intervals. Luckily, the other four fingers on the hand seem to be working OK, so she hadn't dropped anything. As the tech support team got involved, they invoked the logging function on the RTA and shot the data stream to their central pod in Harbin. Careful analysis and a good deal of creativity revealed that the episodes were occurring at exactly 01:00, 02:00, 03:00, 05:00, 07:00, 11:00, 13:00, 17:00, 19:00 and 23:00 – California time! It was obvious that these were prime numbers imposed on a 24-hour clock, and the use of California time strongly suggested that one of the resistance cells left in the old "USA" (now Meiguo) might be involved. Some of those troublemakers simply couldn't get over the change of administration and language that had occurred over three generations ago when the old People's Republic had finally won control of the entire "North American" (Bei Mei) continent (now the provinces of Tsianada, Meiguo, and Wusike) using effective asymmetric warfare and established the People's Empire. The barrage of cyberattacks launched against the critical infrastructure of those countries had effectively shut down their entire civil and governmental rule, leaving the continent easy pickings for the People's Liberation Army invasion.

Dien connected to his office network within a few seconds and accessed the cyber-situational awareness tools that constantly monitored all systems in the empire for possible intrusion or corruption – in addition, of course, to the perpetual scan for disloyal information flows. That side of the dashboard he was visualizing with the input from the network showed the usual sporadic outbreaks of unapproved anti-government propaganda. "Propaganda" was defined as revealing personal enrichment of protected officials, documenting sexual peccadillos by various high-ranking members of the Politburo, and reporting occasional excesses by the PLA leading to excessive deaths (excessive only from the point of view of friends and families of the survivors) in their zealous suppression of treason and revolt at home and in the new provinces.

The dashboard did show, however, that there was a flood of intrusions throughout the Empire that was contaminating the RTAs and causing operational and visual distortions. Most of the reports indicated that the monitors had classified the intrusions as propaganda: people all over the Empire were receiving full access to the private records of the highest-placed officials in the Empire – and there were side-bar reports of growing anti-Empire activity. If the antirevolutionaries' access to the RTAs were not shut down immediately, there could be riots comparable to those of the early 21st century, when failures in the Great Firewall had allowed foreign agitators to foment counter-revolutionary revolts that had led to the death of over 49 million citizens at the hands of the People's Liberation Army. The problem had been that later analysis showed that many of the victims had in fact had nothing to do with any counterrevolutionary activities at all: the PLA had based its actions on flawed information in its databases. Apparently a programmer had been granted access to the databases maintained by the PLA and had accidentally toggled the flag for counter-revolutionary status in some 40 million records without noticing it. The PLA had used the altered records in their house-to-house searches and had executed the corresponding number of innocents as part of their standard operating procedure.

The problem now was that shutting down access to the implants was not easy. Implants were as widespread as the old mobile phones had been in the old days – and everyone depended on immediate access to information that was authorized for distribution by the Empire. Children had their implants installed by the age of two; schooling centered on effective mastery of the devices using neural feedback techniques. In the rare cases where implants had to be shut down or removed, the users found themselves completely isolated from normal interactions. Most people no longer "talked" using their vocal cords once they had their implants; it was so much more effective using the artificial telepathy of the devices for direct contact. The Empire had worked hard to establish the firewalls that prevented the proletariat from accessing leaders' channels so that no inappropriate information would be leaked downwards – and now it looked like those efforts were crumbling.

Dien would have to conference with his colleagues on a high-priority channel to exchange information about the growing crisis. Open access to information was the most dangerous threat to the power structure and the continuation of peace, order and good government in the Empire.

Dien felt the foundations of his world trembling.

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

## **Effective Consulting Teams**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Are you collaborating with colleagues to provide consulting services to clients? Here are some guidelines for working together effectively to serve our clients.

\* \* \*

Consulting services can be structured in two distinct ways:

- We may be providing outsourced services for specific tasks viewed by our client as off the critical path for their primary mission; or
- We may be working to supply an immediate need but with a long-term view to increasing our client's autonomy.

#### **Common Elements**

Every consulting team needs to focus on value to the client. We bring our expertise to bear on specific problems to minimize the long-term costs of providing mission-critical information, improving specific operations, or eliminating specific difficulties. In all these projects, we consultants must *listen* to our clients with great attention and tease out critically important information that our respondents may not even be aware of until we focus their attention on what they may have accepted without question.

On starting our interactions with client personnel, it's crucial to have a clear mandate from upper management – not just the signing officer who ordered the consulting contract – for the work to be done. Taking on a consulting assignment without clarifying the customer's expectations precisely is an invitation for disaster – and a very short consulting career.

In approaching lower level staff, we should make clear that the goal of the consulting work is in no way to harm the interests of any stakeholders and especially not of the employees. Blame and finger-pointing are rarely useful elements of a consulting report – except if we are involved in a forensic investigation about specific abuse, if we are specifically hired to track down the causes of organizational dysfunction, or if our research on some other area of concern brings to light malfeasance or illegality. Usually, though, in my experience operational problems are not rooted in dishonesty but rather in conflicts of purpose, communications and interpersonal style.

One of the tools I have found helpful in my consulting work is what I call real-time notes: even back in the 1980s, I would immediately print out verbatim notes on conversations that I wrote on a laptop computer and give them to the respondent for review. I'd always ask them to let me know of any changes they'd like to make in the notes. Later, in the 1990s, it became much easier to link laptop computers to the customer's workstation screen, so they could actually see what I was writing in the notes in real time. This approach helped reduce anxiety about what I was noting and often resulted in more extended discussions of the issues as the respondent suggested additions (or occasionally deletions) of material.

When performing organizational analyses to detect and resolve interpersonal conflicts, identify under-performing staff or disruptive management behaviour, we often have to cope with a huge

amount of information from many interviews. In 1986, when I had to collate and organize information from over 60 interviews in one organization, I invented Computer-Aided Thematic Analysis<sup>TM</sup>< <a href="http://www.mekabay.com/methodology/CATA.pdf">http://www.mekabay.com/methodology/CATA.pdf</a> > (CATA<sup>TM</sup>), an easy method that allowed me to make sense of about 88,000 facts, impressions, attitudes and behaviours that I had documented in my notes.

Another useful tool I created in the 1980s is Computer-Aided Consensus<sup>TM</sup><
<a href="http://www.mekabay.com/methodology/cac.pdf">http://www.mekabay.com/methodology/cac.pdf</a> > (CAC<sup>TM</sup>), a simple extension of the Delphi Technique<<a href="http://www.seanet.com/~barkonwd/school/DELPHI.HTM">http://www.seanet.com/~barkonwd/school/DELPHI.HTM</a> > to encourage teams of people to generate and then organize as many ideas as they can as quickly as they can.

Both CATA<sup>TM</sup> and CAC<sup>TM</sup> are freely available to everyone and have additional documentation (as narrated available on the METHODOLOGY<
<a href="http://www.mekabay.com/methodology/index.htm">http://www.mekabay.com/methodology/index.htm</a> > page of my Website<
<a href="http://www.mekabay.com">http://www.mekabay.com</a> >.

Within the consulting group, free expression of ideas and opinions is an essential principle. Consulting groups must function under the principles of *egoless work*<
http://www.mekabay.com/nwss/435\_egoless\_work.pdf > as described in the classic work by Gerald Weinberg [Weinberg, G. M. (1971). *The Psychology of Computer Programming*. Van Nostrand Reinhold (ISBN 0-442-29264-3). Xv + 288. Index. Still in print: Silver Anniversary Edition (1998) available on AMAZON via link < http://tinyurl.com/9dk8f >. See pp. 52-60 in particular.] Suggestions for improvement in our methods for serving the client better are to be received with gratitude as contributions to continuous process improvement, not interpreted as personal criticisms.

The team members should be able to communicate immediately with each other, and all such communications must be sent and received using codes that indicate the project involved. For example, a project for, say, Hanofriengo Technologies (a name carefully checked to find that there are no hits for that string in Google!) could be indicated in all related e-mails using a subject line starting with "HT:" All team members must understand that only operationally significant messages are communicated with that prefix; ideally, there would be separate e-mail addresses for personal use by each team member. Thus team members in the Jinbu Corporation would have jinbu.com addresses for work but perhaps communicate jokes and personal news using their individual personal addresses. For more ideas on effective use of e-mail, see "Using E-mail Safely and Well (v4)".< <a href="http://www.mekabay.com/infosecmgmt/emailsec.pdf">http://www.mekabay.com/infosecmgmt/emailsec.pdf</a>>

Consultants should always use digitally signed e-mail communications with their clients and with other team members; there should be no risk of man-in-the-middle attacks sending fraudulent information or instructions that could ruin the project. Communications involving sensitive data such as internal information from the client should be encrypted.

Specialists in the consulting team can play a valuable role only if their specialties are recognized by team members. For example, a marketing consultant's advice on marketing must be acted upon immediately; having a ur-techie dismiss the marketer's advice without a sound basis in successful experience is a waste of time and resources. Similarly, if there's a professional copyeditor in the team, it makes sense to pay attention to her advice.

A Web presence for the consultancy should highlight the organization's strengths in clear language – or in multiple languages – to satisfy potential clients' interests. The Website must be dynamic, with plenty of in-depth resources available at the click of a mouse. Two-layer Websites are too retrograde to generate respect in today's Web-savvy world: each topic should provide

links to on-site resources at increasing levels of detail so that no visitor is left unsatisfied about the specifics of the services offered and expertise potentially brought to bear on their problems. The Website should also be visually stimulating; an example of creative Web design that always impresses me (although I'm biased) is the work of Dave Raimbach of InfoSec Skills<a href="http://www.infosecskills.com/index.html">http://www.infosecskills.com/index.html</a> >, the parent company that runs this blog Website.

#### The Outsourcer

If the consultancy is running a project to fill an unmet need in a client organization, the contract may be long term. Ensuring stability in staffing and providing methods for easy transfer of responsibility to other team members – or even to employees of the client – are important goals for all such work. Even if the client does not foresee internalizing the work currently performed by our team, management personnel and their priorities may change at any time. Having a well-designed transition plan is essential both for the interests of the client and for the reputation of the consultancy. Which verbal report would we prefer: "They left us in the lurch by sequestering knowledge" or "They documented everything for us and provided training for us so that the transition was absolutely smooth"?

#### **Progress Towards Autonomy**

As I wrote in the preceding paragraph, we must be ready in all cases to provide a smooth transition to client control of what we're being paid to do. However, there are many cases where the contract is explicitly designed to ensure that the assignment will not have to be repeated. These jobs have always been the most interesting to me in my career: they provide the opportunity to share knowledge and they usually lead to excellent relations with the client that lead to further – but new and challenging – opportunities for service.

When I founded my own consultancy in 1986, its name was "Jinbu Corporation;" speakers of Mandarin Chinese will recognize Jin\bu\ as meaning *progress*. My company motto, printed on the business cards, was "Progress Towards Autonomy." Many of my contracts included a clause requiring that a specific employee from the client organization be assigned to accompany me in my work for knowledge transfer – an apprentice, if you will. As I performed a security analysis, I'd explain what I was looking for and how I evaluated its implications in a back-and-forth discussion with my apprentice. Many clients called me back for further consulting work, but the projects were always different. It was fun!

I hope that these words of advice will be helpful to young entrepreneurs setting out on their own journey and also to people looking for reliable consultants.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

# **Privacy at Work**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University

Recently I received an invitation to sign a petition:

Think the federal government threatens your privacy? It could be worse -- you could work for them.

Federal agencies are increasingly monitoring their own employees using software that tracks keystrokes, takes screenshots, and even records Facebook and Twitter activity! This threatens employees' abilities to express political opinions and to work freely without fear of censure.

These constitutional abuses came to light when scientists at the FDA, blowing the whistle on unethical drug review practices, found they were being spied on and intimidated. Now it's clear that other government agencies, including the TSA, extensively monitor their employees, down to their personal emails!

How can we expect to live in a free, private society if even federal employees are systematically monitored? Join us in demanding [an] end to federal employee spying.

PETITION TO THE FDA AND TSA: We all deserve the right to privacy, as is guaranteed in the Constitution. We demand that federal agencies adopt constitutional privacy practices and disclose to their employees the extent of monitoring.

I was surprised at the naiveté of this petition.

In my classes on cyberlaw and information assurance management, we discuss the absolute right of employers to monitor, control or restrict the use of the employers' resources by employees. In the United States, the First Amendment of the Constitution is often misunderstood to grant absolute freedom of speech; however, it does not. There are several categories of speech that have been excluded from First-Amendment protection (e.g., sedition, incitement to violence, defamation, and obscenity) but in any case, that constitutional provision applies to governmental restriction of speech in the public sphere. There are many instances where employers – or even customers negotiating contracts with consultants – are perfectly justified in demanding restrictions on speech related to the work being conducted.

Any employer in the USA may define explicit regulations or policies affecting what employees may do with employer-owned communications resources. Typical privacy agreements explicitly state that employees agree to have any communications carried out using employer facilities (telephones, computers, faxes) potentially be monitored or restricted. Non-disclosure agreements provide frameworks to restrict revelation of proprietary or otherwise confidential aspects of an organisation's work. Security levels restrict communications among employees who have different degrees of access; access-control lists and other authorization schemes limit who may access which views of corporate data. Although there are restrictions on monitoring personal

conversations on corporate telephones, it is also possible and legally acceptable to promulgate regulations barring such calls or explicitly letting employees know that all communications using employer-owned equipment may or will be monitored.

An essential component of legality for all such restrictions is that there be no possibility of an expectation of privacy when using corporate resources. Even company cars may be searched legally as long as the policies are clear (privately owned cars may not be searched by employers). The yearly signature of a privacy policy by all employees is one way of ensuring that no one has an unfounded expectation of privacy in the workplace when using corporate tools; on computer systems, a good policy is to post the privacy (or lack-of-privacy) provisions for e-mail, Internet use, instant messaging, and application usage on the login screens for session and even on the start-up screens of applications.

On the other hand, if an employee makes a personal call on a personally owned mobile phone or personally owned computer that is not using corporate networks, normally those calls would be private according to the privacy policies of the organization. Note, however, that any use of the corporate Internet networks would instantly demolish any reasonable expectation of privacy if the policies made that clear.

For a summary of US rulings about privacy at work, see the article "Privacy at Work: What Are Your Rights?" < <a href="http://employment.findlaw.com/workplace-privacy/privacy-at-work-what-are-your-rights.html">http://employment.findlaw.com/workplace-privacy/privacy-at-work-what-are-your-rights.html</a> >. For a review of the European situation, see "European Court of Human Rights Expands Privacy Protections: Copland v. United Kingdom" <a href="http://www.asil.org/insights070806.cfm">http://www.asil.org/insights070806.cfm</a> > and "Personal Privacy in the Workplace: An EU Perspective" <a href="http://mcguirewoods.com/Client-Resources/Alerts/2009/5/Personal-Privacy-in-the-Workplace-An-EU-Perspective.aspx">http://mcguirewoods.com/Client-Resources/Alerts/2009/5/Personal-Privacy-in-the-Workplace-An-EU-Perspective.aspx</a> >.

Please note that I am not an attorney and that the comments above are not legal advice. For legal advice, consult an attorney qualified in the appropriate area of the law and licensed to practice in your jurisdiction.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

## **Sharing a Little Too Much**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University

Recently I was invited to a business meeting using a conference call to discuss a consulting gig with a potential client.

I suggested we use Skype< <a href="http://beta.skype.com/en/">http://beta.skype.com/en/</a>>, which allows us to hear and see each other and also share screens. However, the company sponsoring the meeting uses a different system with similar functions. The software, from a major vendor, provides a virtual meeting room with sections on the screen corresponding to the list of host(s), presenter(s), participants and teleconference information. The main section allows easy screen-sharing.

The first observation that alerted me to security issues with the software was that there was no restriction on who could enter the meeting room. Given a URL in the form < <a href="https://client-company.tool-provider.com/numerical-code/ownername">https://client-company.tool-provider.com/numerical-code/ownername</a> >, the login screen includes two options:

- Enter as a Guest, which asks only for an unauthenticated identifier;
- Enter with your login and password ("required for hosts, recommended for registered users").

There are no restrictions at all on who can use the URL once it is known. Any guest given the URL can resume use of the virtual meeting room at any time and cannot be blocked.

After login, the tool provides teleconference information; in the meeting to which I was invited, there was a toll-free telephone number for linking in by phone. The panel showed the numerical code number used for joining the call; unfortunately, it also showed the code number for the moderator. Thus anyone accessing the panel before anyone else entered that moderator code could take control of the conference call.

The worst aspect of the virtual conference room was that the instant messaging function ("Chat") showed a conversation from several days before between two employees. My contact at the sponsoring company confirmed that there is no automatic method for clearing the chat panel at the end of a conference call. Thus I was startled to see informal comments still on the screen in plain view. Luckily, there was nothing inappropriate or confidential about the text; however, my security-conscious brain instantly imagined a situation where the same meeting space might be used for internal communication – and then made visible to others with no business having access to the internal communications. What if there had been an instant-message discussion of the client on a Friday and that same client logged in on the following Monday? Are all the users of the chat function aware that their texts could be available to anyone logging in at any time?

I discussed the security issues in this product with a helpful member of the product's technical support team.

- There is an option to specify users for a meeting; a popup for host asks for approval.
- There is a feature that allows the organizer to have the system register a user's e-mail address and a specific password created by the host.

- It is possible for the host to provide identical passwords for all participants when sending them password-reset links.
- Once logged in to the system the first time, the registered participants *must* change their passwords themselves.
- The host has no feature available to schedule termination of a meeting.
- The host can delete a specific meeting room at any time.
- The host can create a new meeting room for each meeting.

In discussion with the technical-support specialist, I made the following suggestions to improve the security of the product:

- Require authentication: having an option for security-naïve users that lets anyone log in as a guest without a password is unacceptable. I demonstrated the inadequacy of such a system by logging in successfully as Mickey Mouse. Users who don't routinely think about information security may simply not realize the danger of relying on security by obscurity (knowing the URL for the meeting room) as the only barrier to unauthorized access.
- Virtual meeting rooms with limited lifespan: there *should* be a feature allowing a virtual conference to have a specified termination date and time so that nothing from a specific meeting persists beyond the organizer's preference for termination. If I were designing the human interface, I'd make that a default specification (e.g., all meeting rooms are to be deleted after a specified time) perhaps a time configured by a master administrator so that all meeting rooms run by employees must conform to the organization's standard.
- **Automatic deletion of chat logs:** when a host is about to log off, I would have a *default* popup message warning them that all chat messages will be deleted unless (s)he countermands this process. The notion that possibly confidential internal discussions or discussions with specific clients might be visible to others sends chills up my back.

At the user level, I would not permit such tools to be used in an organization without careful vetting by the security team. No conferencing tool (or for that matter, no software at all) should be in use by employees without approval of the security or information technology group. The responsible experts should formulate specific policies and procedures for using the new tool safely. No user should be authorized to use a tool with potential risks without adequate training.

This experience reaffirms my long-held belief that protecting confidentiality in electronic systems is not a game for amateurs. Every organization designing any product should be integrating security professionals into their development team to identify vulnerabilities and illustrate the range of exploits. Designers need to make security thinking part of their routine, not just something thrown into the mix as an afterthought. Organizations need to take control of their software environment to prevent inadvertent security breaches by their employees.

Sharing is great, provided we know what we're sharing – and with whom.

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

## Managing Information Security Breaches: Studies from Real Life

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University

Michael Krausz < <a href="http://linkedin.com/pub/michael-krausz/0/862/b55">http://linkedin.com/pub/michael-krausz/0/862/b55</a> > is a remarkable young man and a dynamic speaker. He visited Norwich University in November and gave a series of presentations there and at other institutions in Vermont on effective investigations of computer crimes.

Mr Krausz gave me a signed copy of his two books while he was in Vermont. *Managing Information Security Breaches* (ISBN 978-184928-094-5)< <a href="http://www.amazon.com/Managing-Information-Security-Breaches-Michael/dp/1849280940">http://www.amazon.com/Managing-Information-Security-Breaches-Michael/dp/1849280940</a> > is a compact (183 pp) summary of fundamentals of incident response. The AMAZON link provides access to the table of contents.

I think that many readers will be particularly interested in Chapters 7, 8 and 9, which present case studies from small, medium, and large organizations respectively. Each case starts with an entertaining, well-written summary of the situation, continues to the "in-depth explanation" section and ends with lessons learned.

All of the cases are interesting, so I'm picking one pretty much at random. "A case of intrigue – the missing contract" starts with a merger of four companies who hired a managing director. For reasons unknown, the new managing director decided to attack one of the owners by finding information suitable for systematic defamation. The director was fired – and then, due to some legal complexities, fired again. In the period between the firings, the director signed a new contract for himself and for his assistant that awarded them significant new benefits. The two miscreants then threatened to sue their former employer based on these contracts. No one could find the contracts at first; the company laptops – reformatted before they were returned – had been assigned to new users and it took a forensic examination to locate the deleted contracts which, by chance, were on areas of the disk that had not been overwritten. Luckily, the former employees' claims were rejected in three courts.

The author points out that the lack of separation of duties (the "four-eyes" principle) allowed the new director to abuse the resources of his employer. Lack of precise planning for defining the duties of the new director allowed for abuse. There was no adequate termination agreement that could have limited recourse to the courts based on spurious contracts. All the employees had full access rights to their company laptops, allowing the miscreants to reformat their drives. There was no policy requiring anyone to create disk images from the company laptops before they were reassigned. The head of operations had limited knowledge of information technology (IT); his ignorance cause serious delays in locating the deleted information on disk.

Unfortunately, in this case, the company declined to change its culture of total trust, but at least they provided additional training for the employees managing their IT resources.

I very much enjoyed reading *Managing Information Security Breaches* and recommend it as the basis for good discussions in any organization. I am considering it for addition to my reading list in the "Management of Information Assurance"<

<u>http://www.mekabay.com/courses/academic/norwich/is342/index.htm</u> > course I'll be teaching this year.

Krausz has also published a little pocketbook for reference. *Information Security Breaches: Avoidance and Treatment Based on ISO27001*< <a href="http://www.amazon.com/Information-Security-Breaches-Avoidance-Treatment/dp/1849280274">http://www.amazon.com/Information-Security-Breaches-Avoidance-Treatment/dp/1849280274</a> > is a 60-page booklet, perfect for sticking in a pocket, purse or briefcase, that can be used in meetings and discussions or just for thinking about.

#### Good work!

[Disclaimer: I have no financial involvement in Michael Krausz's company or books; I just think he is a brilliant fellow who will continue to contribute to our field.]

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

## **Bidgoli Never MISses a Beat**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Long-time friend and colleague Eddie Rabinovitch is an independent consultant with more than 25 years of experience in IT, networking and security. He is a senior member of the IEEE<
<a href="http://www.ieee.org/index.html">http://www.ieee.org/index.html</a> and an Editorial Review Board member for z/Journal<
<a href="https://enterprisesystemsmedia.com/magazines/z-journal/winter-issue-2012">https://enterprisesystemsmedia.com/magazines/z-journal/winter-issue-2012</a> . He has authored more than 120 papers which have appeared in numerous technical and trade publications. In this book review, he reports on a mutually-favourite author's latest work. Everything below is entirely Eddie's work with minor edits.

\* \* \*

In 2010 Professor Bidgoli
> published his college textbook
<a href="http://www.mekabay.com/nwss/814">http://www.mekabay.com/nwss/814</a> bidgoli mis 2010 (rabinovitch).pdf
> for management information systems (MIS), which at that time I called "the missing link in college education" preparing students for real life applications of information systems. To keep-up with the fast pace of the 21<sup>st</sup> century, since then Professor Bidgoli had published two new editions
<a href="http://www.mekabay.com/nwss/902\_bidgoli\_2nd\_edition\_mis\_(rabinovitch).pdf">http://www.mekabay.com/nwss/902\_bidgoli\_2nd\_edition\_mis\_(rabinovitch).pdf</a> of his excellent textbook, focusing on and emphasizing the most recent developments in information systems management. The most recent edition MIS<sup>3</sup>
<a href="http://www.amazon.com/MIS-3-Printed-Access-Card/dp/1133627307">http://www.amazon.com/MIS-3-Printed-Access-Card/dp/1133627307</a> is yet another gem of a textbook in college education.

As the previous editions MIS<sup>3</sup> is an interactive print accompanied with a full featured eBook educating the readers on the hottest topics and the coolest gadgets and at the same time challenging and engaging them with quizzes and problem solving.

Chapter 1 – "Information Systems: An Overview" describes how organizations use computers and information systems to reduce costs and gain competitive advantage in the marketplace. After studying this chapter the reader should be able to:

- Discuss common applications of computers and information systems
- Explain differences between computer literacy and information literacy
- Define transaction-processing systems
- Define management information systems (MIS)
- Describe four major components of information systems
- Discuss the differences between data and information
- Explain the importance and applications of information systems for businesses
- Discuss utilization of information technologies to gain competitive advantage
- Explain the 5 forces model (buyers, suppliers, substitute products/services, new entrants, rivalry among competitors) for gaining competitive advantage
- Review the IT job market
- Summarize the future outlook of MIS

This chapter, as is the entire textbook, is enriched by real-life examples and case studies from some of the best known corporations; e.g., Hertz, Home Depot, UPS, Walmart, Netflix, FedEx,

and Microsoft. **Case Studies** discuss recent industry trends, such as using IT at FedEx and Mobile Technology for future shopping.

**Chapter 2 – "Computers: The Machines Behind Computing"** describes major components of computers. It reviews the history of computer hardware and software providing a high level overview of computer operations. After studying this chapter the reader should be able to:

- Define a computer system and describe its components
- Discuss the history of computer hardware and software
- Explain distinct factors characterizing computing power
- Summarize computer operations
- Discuss the types of input, output and memory devices
- Explain computer classifications
- Describe the different types of computer software: i.e. operating systems and applications
- List the generations of computer languages

Real life examples in this chapter include companies like IBM and Google with industry connection to IBM and Case Studies discussing Linux as rising OS and Laptop versus Tablet.

Chapter 3 – "Database Systems, Data Warehouses, and Data Marts" gives an overview of databases and database management systems, discussing the history as well as recent trends in database use. After studying this chapter the reader should be able to:

- Define a database and database management system
- Explain logical database design and relational database model
- Define components of a database management system
- Summarize recent trends in database design and use
- Explain the components and functions of data warehouse
- Describe functions of a data mart
- Define business analytics and describe its role in decision-making process

Real life examples in this chapter include companies like InterContinental Hotels Group (IHG). Netflix, Blue Cross Blue Shield (BCBS),Match.com with industry connection to Oracle and Case Studies discussing Business Intelligence and Data Warehouse Applications at InterContinental Hotels Group (IHG) and Data Mining Tools at Pandora Radio.

Chapter 4 – "Personal, Legal, Ethical, & Organizational Issues of Information Systems" examines privacy and ethical issues and discuses reduction of organizational and personal risks. After studying this chapter the reader should be able to:

- Discuss information privacy and methods for improving the privacy of information
- Explain the effects on information privacy of e-mail, data collection, and censorship
- Discuss the ethical issues related to information technology
- Discuss the principles of intellectual property and issues related to the infringement of intellectual property
- Discuss information systems issues affecting organizations, including the digital divide, electronic publishing, and on the connection between the workplace and employees' health
- Describe green computing and the ways it can improve the quality of the environment

Real life examples in this chapter include Verizon's v. OnlineNic Cybersquatting lawsuit, Health and Social issues related to Online Gaming, with industry connection to Anonymizer, Inc. Case Studies are discussing Privacy and Security Breaches at Acxiom and Privacy and other Legal Issues at Google.

**Chapter 5 – "Protecting Information Resources"** highlights awareness, safeguards, and protection of information resources. After studying this chapter the reader should be able to:

- Describe information technologies that could be used in computer crimes
- Describe basic safeguards in computer and network security
- Explain major security threats
- Describe security and enforcement measures
- Summarize the guidelines for a comprehensive security system, including business continuity planning

Real life example in this chapter describes Biometrics at Phoebe Putney Memorial Hospital with industry connection to McAfee. Case Studies discuss The Love Bug Virus and Security Breach at SONY's PlayStation Network.

Chapter 6 – "Data Communications: Delivering Information Anywhere and Anytime" explains the role of data communication systems in delivering information for decision making. After studying this chapter the reader should be able to:

- Describe major applications of a data communication system
- Explain major components of data communication system
- Describe the major types of processing configurations
- Explain the three types of networks
- Describe the main network technologies
- Explain important networking concepts, such as bandwidth, routing, routers, and the client/server model
- Describe wireless and mobile technologies and networks
- Summarize the convergence phenomenon and its applications for personal and business use

Real life examples in this chapter include Cisco's WebEx, Apple's iPhone, and Telepresence as a new use of Data Communication and Convergence. Cisco Systems is the industry connection in this chapter with Case Studies discussing Data Communication at Walmart and Security and Privacy Protection of Mobile Devices.

Chapter 7 – "The Internet, Intranets, and Extranets" introduces the user to the Internet and Web technologies. After studying this chapter the reader should be able to:

- Describe the makeup of the Internet and the World Wide Web (WWW)
- Discuss navigational tools, search engines and directories
- Describe common internet services
- Summarize widely used web applications
- Explain the purpose of intranets
- Explain the purpose of extranets

• Summarize the trends of the Web 2.0 and Web 3.0

Real life examples in this chapter include numerous examples of Internet and WWW applications that became household names. Interesting exhibits in this chapter include IBM's Backbone, Cengage Learning home page as well as experts' predictions on The Internet in 2020, which we should definitely reassess in few years from now. Google is the industry connection in this chapter with Case Studies discussing IBM's Intranet and Social Networking in Support of Small Businesses.

**Chapter 8 - "E-Commerce"** provides an overview of e-commerce and value chain analysis, then comparing e-commerce with traditional commerce. After studying this chapter the reader should be able to:

- Define e-commerce and explain its pros, cons and business models
- Explain the major categories of e-commerce
- Describe the business-to-consumer e-commerce cycle
- Summarize the major models of business-to-business e-commerce
- Describe mobile-based and voice-based e-commerce
- Explain two supporting technologies for e-commerce

Real life examples in this chapter include Twitter's role in helping business to find new customers, USA.gov, e-procurement at Schlumberger, Worldbid.com. Amazon.com is the industry connection in this chapter with **Case Studies** discussing e-commerce applications in online travel and convergence of e-commerce with traditional commerce.

**Chapter 9 – "Global Information Systems"** is dedicated to globalization of information systems. After studying this chapter the reader should be able to:

- Discuss the reasons for globalization and use for global information systems, including e-business and Internet growth
- Describe global information systems, their requirements and components
- Explain the type of organizational structure used with global information systems
- Discuss obstacles to using global information systems

Real life example in this chapter includes Rohm & Haas – part of Dow Chemicals - with industry connection to SAP. **Case Studies** discuss multinational companies challenges dealing with language barriers on the Web and success in global e-commerce.

Chapter 10 – "Building Successful Information Systems" highlights modern systems analysis and design explaining the Systems Development Life Cycle (SDLC). After studying this chapter user should be able to:

- Describe SDLC as a method for development information systems
- Explain the tasks involved in the planning phase
- Explain the tasks involved the requirements-gathering and analysis phase
- Explain the tasks involved in design phase
- Explain the tasks involved in implementation phase
- Explain the tasks involved in the maintenance phase

 Describe the new trends in systems analysis and design, including service-oriented architecture, rapid application development, extreme programming, and agile methodology

Real life examples in this chapter include WestJet Airlines, Sabre Holdings, and Agile Methodology at Overstock.com. CA Technologies (formerly known as Computer Associates International) is the industry connection in this chapter with **Case Studies** discussing **Systems Development at SEB Latvia** and **Crowdsourcing.** 

**Chapter 11 – "Enterprise Systems"** describes enterprise system as an application used in all functions of a business that supports decision making throughout the organization. After studying this chapter the reader should be able to:

- Explain How supply chain management is used
- Describe customer relationship management systems
- Explain knowledge management systems
- Describe enterprise resource planning systems

Real life examples in this chapter include Dell Computer, Time Warner Cable, Amazon.com, Naghi Group with industry connection to Salesforce.com. **Case Studies** discuss ERP and Johns Hopkins Institutions and CRM at Starbucks.

**Chapter 12 – "Management Support Systems"** focuses on improving and expediting decision making process. After studying this chapter user should be able to:

- Describe the phases of decision making process in a typical organization and the types of decisions that are made
- Describe a decision support system
- Explain an executive information system's importance in decision making
- Describe group support systems, including groupware and electronic meeting systems
- Summarize the uses for a geographic information system
- Describe the guidelines for designing a management support system

Real life examples in this chapter include maintenance of electronic health records, electronic meetings at General Motors, and Microsoft Office SharePoint with industry connection to SAS, Inc. **Case Studies** discuss collaboration systems at Isuzu Australia Limited and the increasing popularity of mobile medical-collaboration tools.

**Chapter 13 – "Intelligent Information Systems"** gives a concise, excellent overview of Artificial Intelligence (AI), robots, expert systems, case-based reasoning, fuzzy logic, neural networks, genetic algorithms and natural language processing systems. After studying this chapter user should be able to:

- Define AI and explain how AI technologies support decision making
- Describe an expert system, its applications and components
- Describe case-based reasoning
- Summarize the types of intelligent agents and how they are used
- Describe fuzzy logic and its uses
- Explain artificial neural networks
- Describe how new genetic algorithms are used

- Explain natural-language processing and its advantages and disadvantages
- Summarize the advantages of integrating AI technologies into decision support systems

Real life examples in this chapter include experts Systems in Baltimore County Police Department, Neural Networks at Microsoft and the Chicago Police Department with industry connection to Alyuda Research. **Case Studies** discuss genetic algorithms at Staples and natural language processing making a smartphone smarter.

Chapter 14 – "Emerging Trends, Technologies, and Applications" discusses new trends in software and service distribution, including pull and push technologies, Software as a Service (SaaS), virtual reality, new trends in networking, including grid, utility and cloud computing. The reader also gets an overview of how nanotechnology is being used, its potential and future applications. After studying this chapter user should be able to:

- Summarize new trends in software and service distribution
- Describe virtual reality components and applications
- Discuss uses of Radio Frequency Identification (RFID)
- Explain Quick Response (QR) codes
- Summarize new uses of biometrics
- Describe new trends in networking, including grid, utility and cloud computing
- Discuss uses of nanotechnology

Real life examples in this chapter include Coca-Cola's utilization of RFID-based dispensers for generating business intelligence and cloud computing providers, such as Amazon.com, Google, Microsoft, IBM and salesforce.com, to mention just a few. Mechdyne Corporation is the industry connection in this chapter with **Case Studies** discussing cloud computing's help in cost cuts at universities worldwide and virtual worlds at IBM.

As with its older versions, MIS and MIS<sup>2</sup>, this third edition MIS<sup>3</sup> is a priceless teaching tool for any school of business, science or engineering. It will encourage students to relate the theoretical aspects of different subjects in information systems to real life implementations of these topics.

I also believe, because of the way it's written with a variety of cool auxiliary tools and online references, that this book can be used as a reference guide for popularization and demystification of MIS in any modern business and even at home. It's a perfect teaching tool for non-technical executives moving into any business that is leveraging modern information technology for mission-critical functions.

Congratulations to Professor Bidgoli – again!

\* \* \*

Eddie Rabinovitch< <a href="http://www.linkedin.com/profile/view?id=115837&trk=tab\_pro">http://www.linkedin.com/profile/view?id=115837&trk=tab\_pro</a> is a physicist by training who has more than twenty years of experience in information technology, data processing, networking, security, Internet/intranet/extranet and business communications. He has held executive technical, operational, and consulting positions with major corporations in the USA and overseas in information technology, marketing, business development, program management, pre- and post-sales customer support and is currently serving as a member of the Council of Technology Advisors for the Gerson Lehrman Group (a technology research firm in New York, NY engaged in consulting to major investment and fund management companies).

He has authored more than 120 papers with major technical and trade publications. He is a Senior Member of the IEEE and a frequent speaker at national and international conferences on business and technology.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2013 Eddie Rabinovitch & M. E. Kabay. All rights reserved.

### **Delivery Not Guaranteed**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University

A little while ago a colleague wrote on her Facebook page,

"Just found out that the University is expecting me to teach this semester. Last evening was the first I officially hear of this. I got a strange email from a student in the morning asking about the class, so I contacted the school to find out why a student was asking me. The response was, "Didn't you get the contract back in December?" No, I didn't. Then the comment, "See you on Wednesday for class!" Like in TOMORROW??? OMG! That is why I couldn't sleep."

I added to the thread of shocked, sympathetic comments as follows:

"People don't realize that the definitions of email from the Internet Engineering Task Force Requests for Comments (RFCs) do not include guaranteed delivery. Anyone using email to communicate operationally important information *must* use (a) read-receipts and (b) out-of-band confirmation (e.g., telephone calls) to confirm delivery – and agreement if there's a contract involved!"

The unfortunate incident got me thinking of the wider issue of confirming communications. Supplementary, optional information need not require confirmed delivery, but any operationally-significant information or instruction must have confirmed delivery. Medical offices routinely use an answering message that warns callers not to leave a message if they need emergency help. How would you feel if you had to leave a voice-mail message for an emergency-response team? When the emergency-response operator answers a 999 or 112 call in the United Kingdom or a 911 call in the USA and Canada, every transfer to the appropriate service (fire, ambulance, police) is done with the caller on the line. The caller is immediately transferred to another agent – not told to leave a message.

For technical support and computer-security emergency-response teams, it's essential that the problem-ticket system automatically sends a confirmation message to the client indicating the ticket number for every request for help – a particularly important function when the lines are busy and a client leaves a voice-mail message, or when a client sends a help request through email. With enough exposure to such a policy, clients quickly come to expect the confirmation; if their original request is lost, misdelivered, or ignored, the lack of prompt confirmation from the help desk alerts the client to the likelihood that their message never reached anyone in technical support so they can try again.

When transferring responsibility for a technical-support case from one agent to another, the transferring agent must make person-to-person contact with the agent who will pick up the case; leaving a voice-mail message or sending an email message is not good enough. An interrupted chain of communication will leave a client hanging without support for an indefinite period. An alternative to telephone or in-person contact is instant messaging (IM); an IM request can elicit an immediate response – and failure to respond can prompt further attempts to make contact or

perhaps a switch to a different resource person. In any case, the client will never be abandoned because of an interrupted communication attempt.

Since arriving at Norwich University in 2001, I have consistently refused to accept student essays or assignments on paper. For the first few years, I told students to submit term papers and exams using email; however, a few years ago, when our learning platform became available, I switched to using the intranet functions to upload the assignments to a repository for each assignment. It provides a detailed record of exactly when each student upload his or her file, so there's no ambiguity or uncertainty about whether the student submitted the work on time.

When planning for adjunct faculty staffing, every proposed contract should be confirmed before the contract is sent. My policy would be to make live contact by phone or voice-over IP (VoIP) to ensure that the instructor agrees to teach and accepts the terms of the contract. Then the director of the school or department should send instructions by email to the human resources (HR) group asking for a contract to be sent – and the standard procedure should be that the request is copied to the instructor. The HR group should always send an email confirmation to both the issuing department and to the instructor. If a paper contract is the only format permitted, an HR official should verify that it was received, signed and returned within a reasonable period (say, a week). Lack of response within the stated time would prompt a follow-up call. A checklist would make it easier to ensure that every step of this procedure is completed.

Don't count on luck when interacting on critical issues: verify delivery as a matter of course.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2013 M. E. Kabay. All rights reserved.

#### **Continuity of Operations and the Capability Matrix**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

One of the key principles of business continuity planning is to eliminate single points of failure < <a href="http://www.businesscontinuityuk.net/understanding-the-process/avoid-single-points-of-failure-your-business">http://www.businesscontinuityuk.net/understanding-the-process/avoid-single-points-of-failure-your-business</a> >. Gareth Howell < <a href="http://uk.linkedin.com/in/garethhowell">http://uk.linkedin.com/in/garethhowell</a> > writes,

"Unless the business keeps its eyes on the principles of Business Continuity Management, it can easily get itself into a position where it is overly dependent on the services of a few key individuals. Without proper planning, that dependence can result in disaster if one of those key people is not there." <a href="http://www.businesscontinuityuk.net/understanding-the-process/succession-planning-business-continuity">http://www.businesscontinuityuk.net/understanding-the-process/succession-planning-business-continuity</a>

Mr Howell urges organizations to develop *succession plans* to cope with the sudden unavailability of key people.

"As well as being a good strategy for managing the progression of staff, succession planning is also a good strategy for minimising the impact on the business of losing a critical member of staff unexpectedly. More broadly it seeks to move the organisation to a position where none of its staff actually are critical to its continued operation as individuals." < <a href="http://www.businesscontinuityuk.net/concepts/have-got-succession-plan">http://www.businesscontinuityuk.net/concepts/have-got-succession-plan</a> >

One of the principles I've taught for many years in operations management and security courses can be stated as "No institutional knowledge shall be held by only a single member of the team." Allowing single repositories of operationally significant knowledge is dangerous; one of the classic examples I cite (the reference long since lost in the mists of decades) is of a report published in a USENET group sometime in the late 1980s or early 1990s about a system manager who went on vacation for three weeks on a south-sea island with no external communications. It turned out that critical elements of the operations required knowledge that only he held. The systems were down for the entire period of his holiday.

At one organization where I worked years ago, one of the system managers was a knowledge-hoarder. She kept others from finding out the technical details of how she prevented and solved specific problems, and she refused to document policies so that anyone else could figure out what was permitted and what was not. To find out if something was allowed, the only thing we could do was ask *her*. "Control freak" and "insecurity in action" (in all senses of the word) were kind descriptions for her ham-fisted absolutist control of the production systems. I actually had a talk with the president of the organization in which I warned that – as usual – the only question was when we would have a disaster, not if. Sure enough, a few months after my warnings, the idiot system manager allowed a server to become infected with malware, spreading the toxic code throughout the network. The incident served to demonstrate that not only was she preventing others from taking appropriate security and management precautions, she was actually preventing herself from having her own errors spotted by helpful colleagues.

One of the tools I've long used in evaluating the resilience of organizations is the capabilities matrix < <a href="file:capabilities\_matrix.jpg">file:capabilities\_matrix.jpg</a>. One starts by listing (or brainstorming, perhaps using Computer-Aided Consensus<sup>TM</sup></a> <a href="http://www.mekabay.com/methodology/cac.pdf">http://www.mekabay.com/methodology/cac.pdf</a> ) all the critical functions that the organization requires and all the people in the team. The group then has to decide on a way of rating the capabilities of each person; the figure suggests one way to do it, but in no sense is this suggestion meant to constrain users. The group can come to a consensus on which of the team members can do which tasks at which level of competence and then examine the overall pattern of skills. Figure 1 shows such a matrix with made-up information.

Figure 1. Capabilities Matrix.

								Capab	lities & Assignments		
Total points ≤	0	1	3	6	9	12		0	1	2	3
EVALUATION	ACK!!!	DANGER!	URGENT	IMPROVE	GOOD	EXCELLENT		NO CAP.	NOVICE	IS/CAN BE BACKUP	CAN BE IN
	PERSONNEL CAPABILITIES								DAGRO	CHARGE	
Task	Albert	Betty	Charlie	Dahfla	Edward		Golamo	Hur'dath	TOTAL	NEED	
application monitoring	3	Detty	Charne	3	Luwaru	Панне	2	2	10	GOOD	
application security vulnerabilities	3			3			2	2	10	GOOD	
business impact analysis	Ü	3		1	0	-	-	2	6	IMPROVE	
computer security incident response team	1	3	3		3		2 2	2	8	IMPROVE	
coordination with corporate counsel		3	1		1	2		2	9	GOOD	
		3	1		1	2		2	9	GOOD	-
coordination with human resources group	4	3	1	3	1	2	2	3	9	GOOD	
Database performance	1 2			1.5			8 77 8	- 5	2 5 2	F. F. F. F.	
Database support	2			3			2	2	9	GOOD	1
denial-of-service monitoring				1	3		,	3	7	IMPROVE	
denial-of-service response				1	3			2	6	IMPROVE	
detect cyber-attacks					3			3	6	IMPROVE	_
enterprise antivirus									0	ACKIII	
governance decisions		3	1	1		2		2	9	GOOD	
identification and authentication			2		2		2	3	9	GOOD	
intellectual property protection				2		2		3	7	IMPROVE	
intrusion detection systems					3		2	3	8	IMPROVE	
intrusion prevention systems			2		3		2	2	9	GOOD	
log management systems	1		2	3	3			2	11	GOOD	
manage cyber-attacks		2		1	3	2	1	2	11	GOOD	
monitor dashboard			2	2	3			2	9	GOOD	
network behavior analysis			1	3	2			3	9	GOOD	
network discovery			1	2	2			2	7	IMPROVE	
penetration testing	4 -		1	1	2			3	7	IMPROVE	
quality of service measures	1	3		3	1	2		2	12	EXCELLENT	
respond to system alarms		2	3	1	3			3	12	EXCELLENT	
risk analysis and management				1		3	- /	3	7	IMPROVE	
security awareness	£ .			1	2	3		2	6	IMPROVE	
security information and event management			3	2			2 3	3	8	IMPROVE	
service level agreements	2	3	1	3		3		2	14	EXCELLENT	
system firewalls		3	2	3	3	3	3	2	10	GOOD	
	\$ 8			1	3	3	3	2	6	IMPROVE	
training					3	3	2	3	8		
unified threat management			2		3		-		8	IMPROVE	
vulnerability assessment			2				1	2	-	IMPROVE	
Web site assessment					2		1	2	5	URGENT	
Web site monitoring					3		1	3	7	IMPROVE	
wireless intrusion prevention									0	ACKIII	

In the spreadsheet < <a href="file:capabilities\_matrix.xlsx">file:capabilities\_matrix.xlsx">file:capabilities\_matrix.xlsx</a> I created for this article, I used automatic functions to highlight the danger zones. The red "ACK!!!" flags signal that two functions, "enterprise antivirus" and "wireless intrusion prevention" seem to have been neglected in assignments of duties. Other rows are flagged with other labels such as "DANGER!" up to "EXCELLENT" to give the team suggestions on priorities for improving resilience (overlap of skills).

In addition to simply identifying lacunae in operational readiness, the rows can also alert the team to potential conflicts. For example, if more than one person is rated at the top of the capabilities (in this example, labelled "CAN BE IN CHARGE"), it's important to ensure that the actual assignment of duties is crystal clear. One does not want two people each thinking that they are in charge (leading to potential conflicts) – or for that matter, that the *other* person is in charge (leaving the actual responsibility unfilled). Collegial, friendly discussions can resolve such problems and more important, prevent recurrence.

The column totals are also useful. In the made-up example, the automatic color-coding instantly shows that the lowest score is for Albert and the highest score is for Hur'dath. These scores are *not* inherently good or bad: they just point to outliers. For example, perhaps the low-scoring person is a junior member of the team who needs more training to take up more responsibilities; on the other hand, maybe Albert is a slacker who is shunning productive work. Similarly, maybe high-scoring Hur'dath is a senior member of the team who really ought to be thinking about moving to a more senior position – or maybe he's just overworked and due for a heart-attack.

Users must not make the mistake of thinking that this number-heavy approach is somehow going to make decisions for them – the method is just a heuristic tool to help people *think* about the issues, *decide* on solutions and *act* on their decisions.

Once again, remember my motto: reality trumps theory.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

## Free Emergency-Response Resources from US FEMA

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University

I've been updating a couple of excellent chapters by the distinguished emergency-management expert Franklin Platt< http://www.linkedin.com/in/franklinplatt/ > for the Computer Security Handbook, 6<sup>th</sup> edition, which is due out in October 2013 from Wiley publishers. Frank's work has always impressed me with its thoroughness and professionalism, and I was pleased to be able to pitch in to help update it by checking the current status of all the references. In so doing, I researched the extensive resources he identified at the Web site of the United States Federal Emergency Management Agency (FEMA)< <a href="http://www.fema.gov/">http://www.fema.gov/</a>>, and am pleased to provide readers with an annotated and updated list of pointers to these excellent documents. Mostly I just adapted the tables of contents from the documents themselves, but I think it's helpful for readers to see them all at once. My thanks to Frank Platt for his superb chapters — and while I'm at it, for being the head of the Vermont Chapter of InfraGard < <a href="http://www.vtinfragard.org/about.html">http://www.vtinfragard.org/about.html</a>>.

\* \* \*

FEMA provides extensive resources for Multi-Hazard Mitigation Planning on a wide range of topics and including email updates.

- FEMA Publication 386-1, *Getting Started: Building Support for Mitigation Planning*,< <a href="http://www.fema.gov/library/viewRecord.do?id=1867">http://www.fema.gov/library/viewRecord.do?id=1867</a> > establishes the hazard-mitigation process. Elements include
  - Step One: Assess Community Support
  - o Step Two: Build the Planning Team
  - Step Three: Engage the Public
- Publication 386-2, Understanding Your Risks: Identifying Hazards and Estimating
   Losses, < <a href="http://www.fema.gov/library/viewRecord.do?id=1880">http://www.fema.gov/library/viewRecord.do?id=1880</a> > shows a method of cost-estimating potential losses due to flooding using tables rather than by calculation.
   These tables quickly show that losses can be far greater than expected.
  - Identify Hazards
  - Profile Hazard Events (specific worksheets for each of the following)
    - Flood
    - Earthquake
    - Tsunami
    - Tornado
    - Coastal storm

- Landslide
- Wildfire
- Publication 386-3, *Developing the Mitigation Plan: Identifying Mitigation Actions and Implementation Strategies*, <a href="http://www.fema.gov/library/viewRecord.do?id=1886">http://www.fema.gov/library/viewRecord.do?id=1886</a> > provides guidance on developing the mitigation strategy. Descriptions and worksheets are included for each of the following:
  - Develop mitigation goals and objectives
    - Review and analyse the results of the hazard profiles and loss estimation
    - Formulate goals
    - Determine objectives
    - Get public input
  - Identify and prioritize mitigation actions
    - Identify alternative mitigation actions
    - Identify and analyse state and local mitigation capabilities
    - Evaluate, select and prioritize mitigation actions
- Publication 386-4, Bringing the Plan to Life: Implementing the Hazard Mitigation Plan,
   <a href="http://www.fema.gov/library/viewRecord.do?id=1887">http://www.fema.gov/library/viewRecord.do?id=1887</a> > discusses guidance on implementation.
  - Adopt the mitigation plan
    - Brief local leadership
    - Demonstrate the support of partner organizations
    - Have the plan adopted by the proper legislative or executive authorities
    - Submit your plan for approval
    - Publicize the adoption and approval of the plan
  - Implement the plan recommendations
    - Confirm and clarify responsibilities
    - Begin to integrate mitigation actions |throughout government operations
    - Monitor and document the implementation of your projects and actions
    - Establish indicators of effectiveness or success
    - Celebrate success
  - Evaluate your planning results
    - Evaluate the effectiveness of the planning process
    - Evaluate the effectiveness of your actions
    - Determine why the actions worked (or did not work)
    - Keep the community updated and involved, and celebrate your successes
  - Revise the plan

- Review those factors that affect your community's planning context
- Analyse your findings and determine whether to revise your planning process or mitigation strategy
- Incorporate your findings into the plan
- Publication 386-5, Using Benefit-Cost Review in Mitigation Planning,
   <a href="http://www.fema.gov/library/viewRecord.do?id=2680">http://www.fema.gov/library/viewRecord.do?id=2680</a> > provides heuristics for selecting among mitigation options to maximize cost-effectiveness of expenditures.
  - o Review benefits and costs
  - o Prioritize actions qualitative methods
    - Simple listing
      - List identified actions
      - Identify benefits and costs
      - Assign priority
    - Relative rating
  - o Prioritize actions quantitative methods
    - Simple score
    - Weighted score
  - O Document the review and prioritization process
- Publication 386-6, *Integrating Historic Property and Cultural Resource Considerations into Hazard Mitigation Planning*,< <a href="http://www.fema.gov/library/viewRecord.do?id=1892">http://www.fema.gov/library/viewRecord.do?id=1892</a> > discusses how to work with local planning authorities to protect cultural capital.
  - Organise resources
  - Assess risks
  - o Develop a mitigation plan
  - Implement the plan and monitor progress
- Publication 386-7, Integrating Manmade Hazards into Mitigation Planning,
   <a href="http://www.fema.gov/library/viewRecord.do?id=1915">http://www.fema.gov/library/viewRecord.do?id=1915</a> > explores how to plan for terrorist or criminal attacks in emergency planning.
  - Organise resources
  - Assess risks
  - o Develop a mitigation plan
  - Implement the plan and monitor progress
- Publication 386-8, Multi-Jurisdictional Mitigation Planning,
  <a href="http://www.fema.gov/library/viewRecord.do?id=1905">http://www.fema.gov/library/viewRecord.do?id=1905</a> > emphasizes the importance of collaborative response planning.
  - Introduction
    - What is a multi-jurisdictional hazard mitigation plan?
    - Why conduct multi-jurisdictional hazard mitigation planning?
    - How do you organize a multi-jurisdictional plan?
    - About this document
  - Plan adoption
    - Multi-jurisdictional plan adoption

- Plan participation
  - Multi-jurisdictional planning participation
  - Direct representation model
  - Authorized representation model
  - Combination model
- Planning process
  - Documentation of the planning process
- Risk assessment
  - Identifying hazards
  - Profiling hazards
  - Assessing vulnerability: overview
  - Assessing vulnerability: identifying structures
  - Assessing vulnerability: estimating potential losses
  - Assessing vulnerability: analyzing development trends
  - Multi-jurisdictional risk assessment
- o Mitigation strategy
  - Local hazard mitigation goals
  - Identification and analysis of mitigation actions
  - Implementation of mitigation actions (multi-jurisdictional mitigation actions)
- Plan maintenance
  - Monitoring, evaluating, and updating the plan
  - Incorporation into existing planning mechanisms
  - Continued public involvement
- Publication 386-9, *Using the Hazard Mitigation Plan to Prepare Successful Mitigation Projects*,< <a href="http://www.fema.gov/library/viewRecord.do?id=3388">http://www.fema.gov/library/viewRecord.do?id=3388</a> > is an extensive guide to using all the other resources mentioned above. It is focused primarily on working with the US FEMA.
- FEMA has also developed a *Benefit-Cost Analysis Tool*,< <a href="http://www.fema.gov/benefit-cost-analysis">http://www.fema.gov/benefit-cost-analysis</a> > which assist grant applicants with financial analyses, such as net present value. The same site includes hazard data. Even though it is aimed at US users, it can be helpful to anyone working on financial estimation for risk management.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2013 M. E. Kabay. All rights reserved.

# Are You in Control of Your Data ... or is Your Bring Your Own Device (BYOD) Policy Controlling You?

By: Gordon Merrill, MSIA, CISSP

Colleague and friend Gordon Merrill has been thinking about the issues of integrating personally owned devices into corporate environments. Here is the first of a series of articles on this important topic. Everything below is Mr Merrill's work with minor edits and additions from Mich.

\* \* \*

Winn Schwartau < <a href="http://www.etcss.org/speakers/2012-speakers/">http://www.etcss.org/speakers/2012-speakers/</a> >, speaking at the East Tennessee Cyber Security Summit < <a href="http://www.etcss.org/speakers/2012-speakers/">Cybersecurity conference</a> in October 2012, stated that by the end of 2020 there are expected to be 20 billion endpoints on the internet and by the end of 2050 there will be one trillion. Currently there are over 3,800 versions of just the Android mobile-device operating system < <a href="http://www.android.com/">http://www.android.com/</a> in use. A February 2011 report < <a href="http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#smartphoneos">http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#smartphoneos</a> > estimated almost 500 million shipments in 2011 of new smartphoneos using Android, iOS, Symbian, BlackBerry, Bada, Windows Phone and others.

In 2011, I wrote a series of articles for *NetworkWorld's* "Security Strategies" newsletter which recommended information assurance (IA) work groups to help define some new ideas and new technology for protecting the cloud- and mobile-based technologies that are growing in popularity:

- 1. Is the operating system dead? (Jul 4, 2011) < http://www.networkworld.com/newsletters/sec/2011/070411sec1.html >
- 2. Is your company ready for 4G mobile connectivity? (Jul 6, 2011) < <a href="http://www.networkworld.com/newsletters/sec/2011/070411sec2.html">http://www.networkworld.com/newsletters/sec/2011/070411sec2.html</a> >
- 3. Can you comply with court orders for data from the cloud? (Jul 18, 2011) < http://www.networkworld.com/newsletters/sec/2011/071811sec1.html >
- 4. Does your security policy reflect mobility and cloud security? (Jul 11, 2011) < http://www.networkworld.com/newsletters/sec/2011/071111sec1.html >
- 5. Is your company ready for legal holds and compliance with mobility and the cloud? (Jul 13, 2011) < http://www.networkworld.com/newsletters/sec/2011/071111sec2.html >

In my previous articles, I mentioned how there are still more questions than answers with the proliferation of the consumerization of IT and the multitude of new personal devices. Still companies and IA personnel are faced with the ever tightening restrictions of governmental regulations on security, while at the same time the public is demanding to use their own device, under their personal control, to access anything they want, when they want and how they want. How does a company maintain total control of their data from creation to destruction as the US Justice Department (DoJ) insists, with so many devices wanting to access and grab it? Smart Phones are smart in all that they can do and all that they can access for the consumer, but they are still very immature when it comes to letting IA personnel sleep well at night.

The user will expect to connect to your data portal within five seconds max. This is the length of time needed in a very unscientific study done in one of my classrooms to see how long it took students to fully connect to Facebook. Even though Facebook recently admitted to an average of 600,000 hacked accounts a day<a href="http://nakedsecurity.sophos.com/2011/10/28/compromised-facebook-account-logins/">http://nakedsecurity.sophos.com/2011/10/28/compromised-facebook-account-logins/</a>; that is now the standard connect time that the consumer is expecting to achieve when they click on your application and access your data. You on the other hand are not allowed to have any hacks on any day, but the connection time expectations are the same. Your user will touch the icon for the data portal to your company, hope to connect in five seconds and then have full access to all the data they would have access to in the company. Think through this a minute.

What is this mobile device doing with a portal to your system and data? There is a link between you and them which may or may not be a VPN, so how is it encrypted? What data are going to the phone in order to enable encrypted data traffic? Is it a token passed to the device to authenticate the encryption? Can that also be received by someone else who is monitoring the user's smart device? If not can they still intercept the encrypted transmissions and decrypt later? Even if all of that has been secured by some yet unseen product, now what control do you have on your information after the user gets into it? Can they save it to removable memory; can they resend it from that device to; email, Facebook, cloud storage, Bluetooth devices, printers, fax, or a text with attachment? If they have the ability to do any of the above, have you maintained full control of your data from creation to destruction? According to the US Department of Justice, you have not<a href="http://www.networkworld.com/newsletters/sec/2011/071111sec2.html">http://www.networkworld.com/newsletters/sec/2011/071111sec2.html</a> If you are able to find a way to establish an encrypted connection with no possibility of man-in-the-middle interception with encryption so good it defeats even the Microsoft VPN issues, then you get down to what is left on the device.

So we are left with the following wish list. The user can view all the data they need to make timely business related decision from any deice they choose. The user cannot save the data, forward it, re-post it, print it, or screen shot it (although they can always photograph it with a separate device). And when they are done with their connection there is nothing left on the device that can even be forensically retrieved. So what do we need to make the BYOD have a chance of being anything more than a looming massive data, legal, and financial disaster for any company in the public trust?

So getting back to the basics, what do we want to accomplish despite the failed current models of bring-your-own-device (BYOD)? Users want to access our data for authorized reasons and we need to keep absolute control of our data from creation to destruction. What happens when the user of a BYOD accesses our corporate data and can save them, screen shot them, change them, re-post them, print them or remove them? Have we not then lost control of our data? Yes, we have. Considering that around 17 million mobile devices are lost a year < Winn Schwartau from above >, if there were any data left on the device from our company that could be forensically retrieved, we would have lost control of our data.

Microsoft has the spark of an idea wrapped in one of its features in recent Windows operating systems. We need an application that would allow users to bring their own devices to bear in accessing our data through a view-only application. The screen would only be a remote monitor, a dumb terminal if you will, showing what the user could see if inside the company or at their own desktop. This window would allow them to view, edit, change, and overwrite the data inside the company while the whole time none of that data would ever reside in usable form on or be retained on the device. Again, this technique does not stop side-channel data capture such as photographing the screen and using optical character recognition to regenerate usable data, but it is better than nothing.

In reviewing several potential software vendors for mobile security there is a big gap in how they can secure the data from hijacking (much like a man-in-the-middle attack but worse —making a second phone work on the same frequencies and SIM card channels as the hijacked phone and seeing all the texts, voicemails, data transmissions etc.) or from remaining forensically retrievable data from the mobile device if stolen. I do not see how we can certify remaining in control of our data if they either can be retrieved from stolen device, SIM chip, or recovered from sidetracking for encryption ciphering later. Several companies have software they say allows the smart phone to do some of this now, but they cannot guarantee that while accessing data they did not save it, print it, or copy it, or screen shot it.

Most of the readership of this article will be IT security or IA trained personnel. Even if not certified in Certified Information Systems Security Professional (CISSP), most have been trained in the ten domains of CISSP < <a href="https://www.isc2.org/cissp-domains/default.aspx">https://www.isc2.org/cissp-domains/default.aspx</a> >. The domain of *application security* stresses the need for proper application development to include the overwriting of memory used by this application to keep from leaving behind recoverable or usable data.

So here is where the work groups come in. We can find vendors who will make a form of thin client available as a small form factor virtual desktop. We need to build on that and make the connection secure, a VPN connection and an encrypted connection all within 3-5 seconds. Then we need the connection to allow the user to manipulate his/her internal company "desktop" from their mobile device. Then that "virtual connection" needs to leave all the company data inside the firewall and the "perimeter". When the user

disconnects we need the device to overwrite the memory used per Department of Defense (DoD) standards without a major hit on the mobile device, or battery life. How big is this work group?

The next installment will discuss the legal implications of a BYOD program on the company security program and their potential legal exposure.

\* \* \*

Gordon Merrill< mailto:grmerrill@epbfi.com >, MSIA, CISSP is a cyber security professional whose career spans over three decades and has taken him to 48 states and six foreign countries. Gordon's information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. along with publication of series of articles regarding the skills of an IA professional, the death of the operating system, cybersecurity threats, mobile data issues, and data security. Gordon has been the Chair of the Information Technology department at a local college, and primary instructor for the Bachelors Information System Security Department, instructing students in all ten CISSP domains. Gordon's experience and research have him most worried about eroding personal privacy and lack of potential for real data integrity.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2013 Gordon Merrill & M. E. Kabay. All rights reserved.

#### **Legal Dimensions of BYOD**

By: Gordon Merrill, MSIA, CISSP

Colleague and friend Gordon Merrill has been thinking about the issues of integrating personally owned devices into corporate environments. Here is the second of two articles on this important topic. Everything below is Mr Merrill's work with minor edits and additions from Mich.

\* \* \*

Last time we reviewed some of the implications of bring-your-own-device (BYOD). Today we look further into legal aspects of BYOD.

To date we have not had a major BYOD case to be tested in US courts so security specialists across the water in the US are not sure how it will be interpreted and how the fault and damages will be assigned in cases of security violations based in BYOD.

We can, however, look into one of the tenets of protection most companies rely on heavily and that is the widely used policy of *no expectation of privacy* nearly all personnel are forced to accept to be hired.< http://www.justia.com/employment/docs/workplace-privacy.html >

In the case US vs. Long (2006),< <a href="http://www.armfor.uscourts.gov/opinions/2006Term/05-5002.pdf">http://www.armfor.uscourts.gov/opinions/2006Term/05-5002.pdf</a> the US Marine Corps searched the official email records of Lance Corporal Jennifer N. Long, USMC, and scanned through a large assortment of her emails to find some incriminating evidence:

Appellee was charged with several specifications of unlawful drug use in violation of Article 112a, Uniform Code of Military Justice (UCMJ). The Government's case was based, in part, on several e-mails that were sent and received by Appellee and that were retrieved from a government server. These e-mails contained statements written by Appellee indicating, among other things, a fear that her drug use would be detected by urinalysis testing and the steps she had taken in an attempt to avoid such detection.

At trial, the defense made a motion to suppress the e-mails because they were the result of a search which was not properly authorized. The military judge denied the motion holding that Appellee had no expectation of privacy in the e-mails stored on the government server. Contrary to her pleas, Appellee was convicted by members of the charged offenses. On appeal, Appellee challenged the ruling of the military judge on the motion to suppress her e-mails. The United States Navy-Marine Corps Court of Criminal Appeals disagreed with the military judge, holding that the search was unlawful, but further concluding that the error in admitting the e-mails was harmless beyond a reasonable doubt.

The Marines thought they were golden because they had the user sing a "no expectation of privacy" agreement as well as having a splash screen pop up on every log in. What the court found was remarkable and I will merely list some of the key points.

- They found the defendant *did* have a reasonable expectation of privacy (EOP). They compared it to a high school locker. All high schools retain the right to break the lock if ordered by a police officer, but when a student returns to school and their lock is in place they assume their locker contents are still secured.
- Despite the logon banner which said otherwise, the court found the user did still have a

- degree of EOP, and she also had no recourse but to click OK in order to do her job.
- Because the email sat behind a password only she knew, they also agreed that she should reasonably expect that no one else was looking at her email: it was not public and no one should be able to access it without her password.

The next two points are key and I think where most companies are not prepared to cover their assets.

- The court said the users' "EOP depends on the facts and circumstances at the time" which differs greatly from the form most people sign and companies rest and rely upon.
- They also said the definition of "EOP is equal to that which "society is willing to accept as reasonable."

The court determined that society was willing to accept that users should have the expectation of privacy, even at work, and even on company equipment. As a result, Ms Long's conviction was overturned. Even when carrying out a legal discovery order from a court, if you do not carry this out properly, you can go to jail yourself for illegal discovery.

Additional findings that led to that decision by the Court included

- The Marine Corps is part of the US government, not a private business.
- Administrators searched the entire mailbox rather than doing keyword searches.
- The search was not a normal maintenance process consistent with *official* policy.
- Maintenance procedures did not call for the review individual email items.
- These emails were collected on behalf of law-enforcement authorities without warrant. This situation made the office staff deputized agents subject to Fourth Amendment restrictions on search and seizure.
- Emails used for the prosecution were thus obtained improperly.
- This situation left the case with constitutionally inadmissible evidence.
- Because of the bad evidence, the drug conviction was also overturned and a rehearing authorized.

Several questions are raised by this case for private employers:

- Do your security and forensic policies address proper procedure to prevent employees from working as deputized agents of law enforcement without authorization?
- Are you monitoring compliance with official policies to prevent development of "policy by practice?"

A good example of policy by practice was in a Fortune 250 company whose official security policy required all users of their virtual private network to authenticate using two-factor authentication. However, in practice the information security department never used the two-factor authentication – they only used one, if that. That practice was a known operational process that was unchallenged for more than six months. That sloppy authentication became the *policy by practice*, legally, and then had to be defended by the corporate legal team in court cases.

Most of the companies who will be large enough to anticipate a BYOD rollout will be large enough to fall under various compliance regulations for corporate and individual data security.

As governmentally mandated deadlines approach, the lack of solutions to ensure compliance in a BYOD environment is a serious source of concern for security professionals.

The problem for most IA personnel is the lack of perceived need by corporate upper-level managers. In this current economy, the word from the C-level is all too often, "do the minimum." In their book, *Building a Career in Compliance and Ethics*< <a href="http://www.amazon.com/Building-Career-In-Compliance-Ethics/dp/0979221021/">http://www.amazon.com/Building-Career-In-Compliance-Ethics/dp/0979221021/</a> > authors Joseph E. Murphy and Joshua H. Leet state.

"The line between what is unethical and what is illegal is sometimes blurry and unpredictable. If a company seeks to scrape by doing the minimum the law requires, the odds are fairly high that it will fail in this goal. Those who aim for the bottom tend to miss their low target and eventually break the law."

The problem with that approach is that IA personnel can be blocked by the C-level's lack of support and backing. An article in *Infosecurity Magazine* from 13 November 2012 < <a href="http://www.infosecurity-magazine.com/view/29293/most-companies-allow-byod-instead-of-maximizing-it/">http://www.infosecurity-magazine.com/view/29293/most-companies-allow-byod-instead-of-maximizing-it/</a> pointed out that

"Eighty-eight percent of users believe their mobile devices are at least relatively secure; but 77% of IT managers see the risk of malware spreading to the corporate network from mobile devices as moderate to very high. The result, caught in the cross-fire of desire from the users, and fear of security for the business, is often a policy that is both insecure and inefficient."

Lack of support from upper management can seriously undermine the information security personnel's exercise of their knowledge and judgement.

I think one of the recent quotes I have heard that summarizes this situation the best is from Geoff Web.< <a href="http://www.infosecurity-magazine.com/blog/2012/11/16/mobility-cloud-and-elephants/695.aspx">http://www.infosecurity-magazine.com/blog/2012/11/16/mobility-cloud-and-elephants/695.aspx</a>>

"Whether it's accessing a SaaS application from your desktop, or a consumer cloud storage provider from your smartphone, the goal, and the challenge, is the same: get my users access to the data they need, and keep everyone else out. Everything else is window dressing. We can't afford to make the mistake of focusing on one element at the cost of the others. Devices, services, mobility – are simply the details; the real challenge is keeping data available and secure."

I have not seen a BYOD policy yet that I feel safe enough using, trusting it to keep me out of jail. Mobile device management (MDM) options I have seen to date are a sure way to turn BYOD into Bring Your Own (Legal) Disaster. Work groups are needed to recreate how BYODs connect in order to make this anything but business and legal Russian roulette, and none of this is possible with "give me the minimum."

\* \* \*

Gordon Merrill< <a href="mailto:grmerrill@epbfi.com">mailto:grmerrill@epbfi.com</a> >, MSIA, CISSP is a cyber-security professional whose career spans over three decades and has taken him to 48 states and six foreign countries. Gordon's information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. along with

publication of series of articles regarding the skills of an IA professional, the death of the operating system, cybersecurity threats, mobile data issues, and data security. Gordon has been the Chair of the Information Technology department at a local college, and primary instructor for the Bachelors Information System Security Department, instructing students in all ten CISSP domains. Gordon's experience and research have him most worried about eroding personal privacy and lack of potential for real data integrity.

For the slides he recently used in a presentation at a chapter meeting in Chattanooga, Tennessee for the Information Systems Security Association (ISSA) about these topics, you can download a PDF version of the PowerPoint deck.<

http://chattanooga.issa.org/wp-content/uploads/2013/02/ISSA-CHA-BYOD.pdf >

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2013 Gordon Merrill & M. E. Kabay. All rights reserved.

#### Mid-Term in IS342: Questions from Upper Management

The IS342 Management of Information Assurance course <

<u>http://www.mekabay.com/courses/academic/norwich/is342/index.htm</u> > is halfway through this semester's work. At mid-term, I provide a mid-term multiple-choice exam and also give students a couple of weeks to respond to memos supposedly from high-level executives to them as if they were Chief Information Security Officers (CISOs) in industry. Their essays are graded simply on a 10–9-8–0 scale:

- 10: This is great! Could even be published!
- 9: Good work. Solid, concise, no significant errors.
- 8: At the limit of professional acceptability has a few grammatical or spelling errors or some minor imprecision
- 0: Unacceptable: factual errors, rudeness, disruptive bad writing....

I was so pleased by the responses written by student Gregory Antonellis to the current mid-term memo-exam that I have obtained his permission to publish his memos.

\* \* \*

1. FROM: Edward J. Olmos, Director of IT Operations

TO: YOU as CISO

RE: Using MacroHard Wurd on multiple systems

Hello. I'm sorry to tell you that your recent actions have caused quite a ruckus in the IT department. I know that you were recently an ISSO in government service, but you have to understand that things are different here at the Lurwatzer Corporation. We bought the master copy of MH Wurd at Staples perfectly legally. We own that software now, so we installed it on all 827 workstations running MH FrenchDoors v11, as we are entitled to do. The Wurd package cost us over \$430, so I think you will understand that we've paid our fees for the product and can use it freely inside our corporation as long as we don't allow our employees to bring copies home to their personal computers. We do obey all laws and principles of ethical behavior here. So in conclusion, I think you're going to have to back off this ridiculous proposal for us to pay \$3,000 for a "site license" that supposedly covers up to 1,000 installations in an organization. We can use the money for better purposes than that.

FROM: Gregory Antonellis CISO

TO: Edward J. Olmos, Director of IT Operations

SUBJECT: re: Using MacroHard Wurd on multiple systems

Mr Olmos,

I'd like to state that I'm sorry if my actions have disrupted the IT dept. I believe you are very mistaken about our use of MH Wurd on company workstations. We do not own that software. We own a license to use a copy of it. To use the software in a way that violates said license gives the publisher grounds to file a lawsuit against Lurwatzer Corporation in civil court and may also be a violation of civil law. I assure you, installing a retail copy of MH Wurd on over 800 workstations is definitely in violation of the license agreement with which that product was sold, seeing as MacroHard does not sell volume or site licenses in retail form. The various licenses available in retail stores allow installation on between one and ten workstations. Whether or not these workstations are internal, external, privately owned or on Mars makes no difference a violation of the license is still a violation of the license, which is grossly unethical. I stand by my statement that we purchase a site license. I am of the belief that safeguarding the

company from a lawsuit and the effects that lawsuit would have on our reputation is a perfectly good purpose for which to allocate \$3000. If this is not possible then we should reconsider our use of MH Wurd and consider more affordable alternatives. If you feel I have made these statements in error, please contact me so we can arrange a time to meet in person.

Sincerey, Gregory Antonellis, CISO

\* \* \*

2. FROM: Mary McDonnell, CIO

TO: YOU as CISO

RE: Software development project

Thanks for your excellent presentation yesterday on your proposals for how to start our first internal software development project. This is pretty exciting, because it's only recently that we have seen a cost/benefit ratio that justifies our hiring our own programming team to write our very own software for a competitive edge. I think that the neural network our team is sketching out will really provide a tremendous boost to our data analysis capabilities for sales and also for customer support. The reason I'm writing is that I'd like you to flesh out your brief mention yesterday about defining our current system as a production system and building a new development system. Can you explain why we shouldn't just have the development team do all their work on the system where their software will ultimately run? Why should we buy and install a separate one? Oh yes, and you also mentioned separation of duties during your talk, but I don't see how that applies to the software project or is related to the new system.

FROM: Gregory Antonellis CISO TO: Mary McDonnell, CIO

SUBJECT: re: Software Development Project

Ms. McDonnell,

In response to your questions about my presentation: A production system is a system that performs a critical function for our organization; basically, it's any system that would disrupt business as usual if it broke. A development system is a system that is as equivalent as possible to a production system but is not actually performing a task for the organization. The purpose of a development machine is to provide a safe environment to test any changes to a production machine before we make them to the production machine so that if the changes break anything our actual production machine is unaffected. Separation of duties is relevant to software development because it allows for more secure code. By having the software written and tested by different people we can ensure that there are no unauthorized additions to the code and no shortcuts were taken. We can also that testing is thorough. If the same people write and test the code there's a possibility that testing will may not be thorough if the testers assume that "we know we wrote that section right so there's no need to test it." I hope this answered your question, if not, please feel free to contact me.

Sincerely Gregory Antonellis, CISO 3. FROM: Jamie Bamber, VP Marketing

TO: YOU as CISO RE: Ethical problem

Hi! Mary McDonnell and Eddie Olmos both suggested that I discuss a current issue with you because, they said, you come from a university with strong emphasis on ethics. Here's the scoop: Jamila is working on a new advertising campaign to counter the most recent release of Yontraubon Industries' GzornoGood<sup>TM</sup> gzornoplatzes. As you know, we've been neckand-neck with that company for the last six years in the same market, and our GreatGzorn product really needs a marketing boost. Well, it turns out that Jamila's boyfriend's sister's husband works at Yontraubon as a Senior VP of Marketing and is really irritated at the way he's been treated in the last year. He was supposed to get a major account from his boss but instead his boss gave the account to the boss' own mistress!! Isn't that appalling? Anyway, this guy is ready to jump ship and join our company right away — and the best thing is that he is willing to bring us inside information about the next generation of GzornoGood<sup>TM</sup> gzornoplatzes! With that information, which includes some schematics and test data, we can get our own GreatGzorn's out by next September with even more features and at half the cost (since we won't be paying for the research and development that went into the GzornoGood<sup>TM</sup> plans). I was all set to go with this move, but Mary and Eddie said I really should ask you for your analysis of the ethical issues. I hope you can have your response ready within a day or too, 'cause we're really hot to trot here!

TO: Jamie Bamber, VP Marketing

CC: Jamila <u>lastname</u> here

FROM: Gregory Antonellis, CISO Subject: **URGENT:** Ethical problem

Mr. Bamber,

If we were to acquire intellectual property information via his insider knowledge it would be highly unethical and potentially illegal depending on the intellectual property involved. I recommend that we do not accept any proprietary information from this guy. I also recommend that we do not make any effort to contact this person. If he's so willing to jump ship so readily he could pose a risk to our company as well. Please tell Jamila that she shouldn't under any circumstances accept insider information her "father's brother's nephew's cousin's former roommate" (or whatever the relation is). Unless legally or ethically required to do otherwise, we should NOT follow up on this and ignore any correspondence from this individual if he does contact us. Considering that my knowledge of this situation is limited to what you emailed to me, I would recommend not yet turning him in to the management at Yontraubon Industries. I believe that's the "safest" move for all parties right now, seeing as it's possible that he's all talk. If it turns out he is actually willing to put his money where his mouth his he should be able to sink his own ship without our help. As I said, my knowledge of this situation is limited to what was in your email. Please keep me up to date on any developments.

Sincerely, Gregory Antonellis, CISO

\* \* \*

4. FROM: Tricia Helfer, HR Director

TO: YOU as CISO

RE: Telling us what to do in our own email

I'm sorry to tell you that your memorandum about changes in our email policy are not going over very well with many of the older employees. I've received complaints with the following criticisms, and I need your expertise to explain to these people why you are acting as you are:

- Why are you telling us that all our corporate email can be examined at any time, for any purpose, by authorized personnel in the IT and the Security groups? Surely our email is our own, even if it's on the company servers?
- What's wrong with using old email messages as a way of starting new conversations? You just haul up an old message and hit REPLY ALL simple, no?
- Why have you written that "Operationally significant and urgent information must NOT be consigned to email, or if it is, deliver must be confirmed in-person, by telephone conversation (not voicemail), or real-time instant messaging."
- Why can't our employees decide what email to delete without having to consult some sort of policy documentation? What's wrong with just keeping and deleting what our users they are the experts in their own area, you know feel should be kept or deleted?

FROM: Gregory Antonellis CISO TO: Tricia Helfer, HR Director

SUBJECT: re: Telling us what to do in our own email

Ms. Helfer,

I understand that you've received several common complaints about the revised email policy for which you would like explanation. I've copied the questions from your original email and included an answer below each.

• Why are you telling us that all our corporate email can be examined at any time, for any purpose, by authorized personnel in the IT and the Security groups? Surely our email is our own, even if it's on the company servers?

Company email is reasonably analogous to company letterhead, as communications made with company resources with company branding it is company property, not personal property. As company property, authorized personal need to be able to access it if necessary. If employees would like to use email for personal purposes they should use personal email (provided such use is in compliance with company policy) but should be aware that their use of personal email via the company network or company owned hardware, while still their property, is less private than if they were to do so using their own hardware and resources.

• What's wrong with using old email messages as a way of starting new conversations? You just haul up an old message and hit REPLY ALL – simple, no?

There are two reasons this is not correct. If one simply replies to an old message when starting a new conversation the subject line will not reflect the subject of the new conversation. Furthermore, it would be inappropriate to carry out an important email exchange (e.g. a discussion about product design) in reply to an email with a less critical topic (e.g. trading company furniture) and vise-versa. If done repeatedly, recipients quickly learn to ignore the subject line. This can cause important information to be ignored on the premise that the subject has nothing to do with the message. Secondly, the REPLY-ALL feature should only be used when every person needs to be direct recipient of an email. It is not a catch-all replacement for the proper use of the CC and BCC fields. Over use of REPLY-ALL quickly leads to the intended recipients of email disregarding messages on the premise that they are not actually of relevance. Replying to old messages with REPLY-ALL combines the effects.

• Why have you written that "Operationally significant and urgent information must NOT be consigned to email, or if it is, deliver must be confirmed in-person, by telephone conversation (not voicemail), or real-time instant messaging."

Operationally significant and urgent information mustn't be consigned to email unless delivery is properly confirmed because, **just like physical mail** there is no guarantee that the recipient will check their mail, open it, actually read it, pay attention reading it, all in a timely manner.

• Why can't our employees decide what email to delete without having to consult some sort of policy documentation? What's wrong with just keeping and deleting what our users – they are the experts in their own area, you know – feel should be kept or deleted?

I truly understand the inconvenience of this policy, but it simply is not in our control. In order to comply with various laws, standards and regulations involving healthcare, product liability, protection of intellectual property, accounting and taxes we are required to keep various types of information and the relevant communications (e.g. email) about that information for various lengths of time. I understand that our employees generally know what should be kept or deleted (as you said, they are the experts in their own areas), but we are legally required to comply with regulations regarding data storage and disposal. Please be assured that the IT dept. isn't making everyone's lives harder on a whim, we'd just rather not see steam come out of some bureaucrat's ears for not doing so.

I hope I have answered these questions in a way that's adequate for your use. If you have any further concerns please feel free to contact me.

Sincerely, Gregory Antonellis, CISO

\* \* \*

**Notes from Prof Kabay about the Author:** Gregory Antonellis<mailto:

gantonel@student.norwich.edu > is from Massachusetts and is enrolled in the Bachelor of Computer Security and Information Assurance (BSCSIA) program at Norwich University. He entered Norwich with Advanced Placement College Board courses in Calculus, General Physics I and General Physics II. He already has extensive experience in programming and was exempted from taking the introductory first-year programming courses, going directly into second- and third-year courses in his first semester. He took five courses instead of the required four in his first semester, and is taking six courses instead of the required five this semester. I am proud of how Norwich University supports our gifted students and expect to see Mr Antonellis contributing significantly to our field. Anyone interested in offering Mr Antonellis internships is welcome to contact him directly!

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2013 Gregory Antonellis & M. E. Kabay. All rights reserved.

## **Prescription for Failure**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University

One of the concepts I've always enjoyed pointing out to my young students is the *side channel*. We were just discussing monitoring and control systems in the IS342 Management of Information Assurance< <a href="http://www.mekabay.com/courses/academic/norwich/is342/index.htm">http://www.mekabay.com/courses/academic/norwich/is342/index.htm</a> > course (PPTX slides<

http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch53\_monitoring\_control.pptx > and PDF notes<

http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch53\_monitoring\_control.pdf > freely available) and one of the issues that came up was how to indicate a problem in a monitored system. "If we're monitoring the network and it goes down, how do we tell anyone it's down?" The students rightly piped up, "Use another communication medium" and we discussed walking over to tell someone, posting a paper note as a warning, generating robotic voice status updates via phone, sending text messages using SMS (Short Message Service) to mobile phones, putting information on electronic dashboards for situational awareness using separate networks, and other side channels.

Another case where side channels play an important role in *breaking* security is data-loss prevention (DLP)< <a href="http://csrc.nist.gov/groups/SNS/rbac/documents/data-loss.pdf">http://csrc.nist.gov/groups/SNS/rbac/documents/data-loss.pdf</a> >. A primitive DLP is the Acrobat security feature that can lock a file against copying or printing by using a password to allow such functions. Unfortunately, the password security is weak; entering "crack acrobat password" into a search engine brings up thousands of hits for free or commercial password-cracking software tailored to attack secured PDF files.

Some DLP systems use kernel-level modifications to prevent such functions as copying, modifying, printing, email, screen captures and so on. For example, McAfee Data Loss Prevention software< <a href="http://www.symantec.com/data-loss-prevention">http://www.symantec.com/data-loss-prevention</a> > provides control over

- Input/output (I/O) involving removable media such as flash drives;
- Restricting what can be attached to email messages;
- Blocking printing on all but specified printers;
- Controlling uploads to Websites;
- Blocking the use of screen captures.

Unfortunately, none of these products can stop a disgruntled employee turned industrial spy from snapping a photo of a screen or printed page full of valuable, confidential information using her mobile device camera. Even ordinary cell phones now have unprecedented pixel densities; for example, the Samsung Galaxy Note II has a back-facing camera that provides 8 megapixels. I didn't even bother looking further for the even higher density devices I'm sure exist already or are coming soon.

Beyond photographs or movies, cell phones and tablets have microphones: it is trivial to initiate a recording and then slip the screen-darkened phone into one's carrying case or jacket pocket.

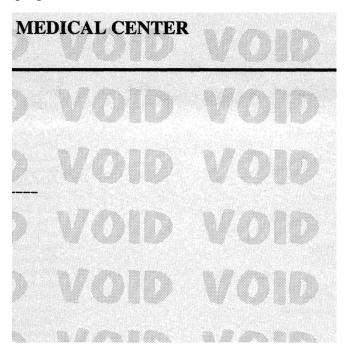
There's a reason that organizations using sensitive compartmented information facilities (SCIFs – see for example SCIFSOLUTIONS< <a href="http://scifsolutions.com/">http://scifsolutions.com/</a>>) complement their Faraday cages with strict rules on exactly what electronic equipment is permitted past the security guards at the entrance to the secured portions of the building. The whole point of a SCIF is to prevent unauthorized data leakage using side channels; allowing someone secretly to record a top-secret conversation with a cell phone would be silly.

A classic use of side channels is steganography<

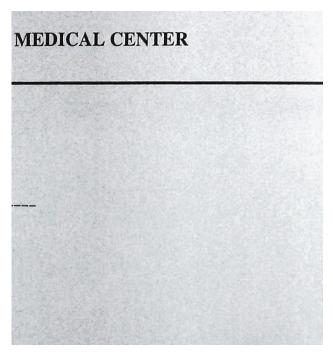
http://www.garykessler.net/library/steganography.html >, which refers to hidden writing — information transfer in non-obvious forms such as integrated into music, photographs, videos, Web pages and so on. Unlike cryptography, which alters cleartext into ciphertext that is usually immediately obvious, steganography conceals even the existence of the message. A microdot could be considered a steganographic technique, since unless one knows which dot on a printed page is actually a microphotograph readable through a microscope, one is unlikely to know that there's a secret message at all.

Recently I discovered a failed form of DLP when I was given a prescription during an unfortunate visit to an emergency room (I have ripped my right leg's hamstring muscle with agonizing consequences). I scanned the prescription so I could send it to my wife (since I can't drive now) by email (because I forgot to give it to her when she left in the morning) to pick up a pain-killer that won't make me crazy (I become agitated and violent when given ordinary narcotics)(really). Here's a section of the resulting scan< prescription\_scanned\_close-up.jpg >:

This is great, right? The actinic light of the scanner brought out a completely invisible marking to warn pharmacists that someone is presenting them with a copy of a prescription – a copy possibly modified for evil purposes.



Unfortunately, the method is limited. Here's the same area of the paper photographed in ordinary fluorescent light on my desk using my cell phone camera< prescription\_photographed\_close-up.jpg >:



Oops. No VOID marks.

I'm reporting the problem to the head of the pharmacy at the hospital, with a request that the alert be passed up the chain to the people who (a) created the paper and (b) ordered it to be used for prescriptions.

There are many methods for making paper difficult to duplicate; experts who manage the money supply< <a href="http://www.moneyfactory.gov/anticounterfeiting.html">http://www.moneyfactory.gov/anticounterfeiting.html</a> > have invented high-resolution printing with subtle colours, insertion of plastic bands with authenticating information, and so on. All of these cost extra, but at the very least, the people who created the non-copy paper should have checked the possibility of a simple photograph in ordinary light before releasing their special product.

Failing to think outside our preconceptions is a prescription for failure.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2013 M. E. Kabay. All rights reserved.

#### PRAGMATIC Security Metrics: Applying Metametrics to Information Security

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University

Recently I was surprised to be asked to write the Preface to a new book: W. Krag Brotby and Gary Hinson's *Pragmatic Security Metrics: Applying Metametrics to Information Security* (CRC Press – Taylor & Francis Group, 2013 (ISBN 978-1-4398-8152-1; xviii + 494; index)<a href="http://www.amazon.com/PRAGMATIC-Security-Metrics-Metametrics-Information/dp/1439881529">http://www.amazon.com/PRAGMATIC-Security-Metrics-Metametrics-Information/dp/1439881529</a> >. After reading the galley proofs, here's what I wrote (using US spelling):

Information assurance (IA) has suffered for decades from the lack of sound quantitative methods for coping with risk and evaluating alternative strategies for allocating resources wisely in the fight against errors and attacks on our information systems.

All of us involved in IA maneuver through competing frameworks for choosing and implementing defenses; unfortunately, all too often we rely on the equivalent of word-of-mouth recommendations – industry best practices – in choosing particular paths. As our field matures, we must learn from other professions where methods for evaluating the quality of approaches have shifted from purely intuitive approaches to more systematic and repeatable methods.

The authors of this book have contributed their experience and creativity to present a valuable methodology for creating and evaluating elements of security management. Throughout the work, they emphasize how important it is to use heuristics rather than rigid rules in any field that changes constantly.

Security of all kinds suffers from the fundamental difficulty that if security measures work, there's less evidence that the measures were necessary, at least for non-professional observers such as non-technical managers. Without sound metrics, we are in the position of passersby who encounter a man swinging plucked chickens around his head while he stands on a street corner: asked why he is doing that, he answers, "To keep the flying elephants away." "But there are no flying elephants," respond the befuddled observers. He crows triumphantly, "See? It works!"

Without defining, testing and refining metrics, our profession will continue to be subject to the legitimate question, "How do you know?" How do we know if our proposals – our proposed spending, our proposed topology, our proposed changes – are reasonable? Why do we choose one set of responses over another? And how will we measure the results of our methods to evaluate their effectiveness and their efficiency?

In addition to supporting the development of IA, the methods presented in this text will reach professionals in fields that will benefit from good, PRAGMATIC metrics.

Thanks to Krag Brotby and Gary Hinson, I expect to see dramatic changes in our ability

to analyze our security options, explain our choices, and measure our results.

I received my free copy of the book a few weeks ago and want to let readers know about it. I really like the "Office Memorandum" on pp xvii & xviii, which looks like one of my own examination questions: it's a request from a chief executive officer to the information security manager and it asks for a written explanation of

- What's the return on investment of the spending on information security over the last three years?
- How does the company's information security program compare with those of comparable companies in their industry?
- Are they spending too much on information security?
- If they have to cut expenditures, what aspects of the information security efforts could reasonably be reduced?

These questions echo those I have insisted for years must be answered at any time by a security manager:

- What are we doing and how much are we spending on information security?
- Why have you decided that we don't need to do and spend more?
- Why have you decided that we don't need to do and spend less?

Answering these questions without methods for measuring our efforts – that is, having *metrics* – is difficult. Without metrics, we're reduced to guesswork and intuition. The authors specifically use the following pragmatic definitions which are interesting in themselves:

- Governance: the act of governing through mandating a set of rules and regulations regarding the actions of individuals within the organization, plus the directive, control, and feedback processes to ensure their compliance.
- Indicator: something that gives an indication, that is, an indirect, vague, and/ or imprecise measure that may not be strongly correlated with the subject of measurement.
- Instrument: short for "measuring instrument," that is, a device for measuring.
- Measure: (verb) to determine one or more parameters of something; (noun) short for measurement, for example, the meter ("metre" outside the United States) is a length measure.
- Measurement: the value of a parameter for something, ideally expressed in defined units with an appropriate degree of precision, for example, "the height measurement of the door is 1.98 meters."
- Metametric: information about metrics....
- Metric: a measurement in relation to one or more points of reference.
- Metrication: the process of selecting and applying metrics to improve the management of something.
- Metrician: a metrics practitioner—someone fascinated with metrics who develops and uses metrics.

In Chapter 2, "Why Measure Information Security," the authors write,

From our experience, we believe there is a genuine and increasingly urgent need for

viable metrics in information security. While, to date, the profession has generally muddled through with almost no rational, sound, and defensible security measurements, the situation is simply not sustainable over the long term. We are fast approaching and, in some cases, already exceeding the limits of the information security manager's gut feeling, qualifications, and experience, coupled with the use of ill-defined and generic good or so-called best practices, as a basis for extremely important security and risk management decisions. While not so common these days, there are still those who contend that as long as you implement best practices, you don't need extensive metrics. However, best practices are an inadequate substitute for genuine knowledge. What may be best in one organization may be too costly and excessive in another or, in some cases, wholly inadequate. Without metrics, how would you ever know?

Brotby and Hinson pose and discuss the following questions in Chapter 2:

- Are we secure enough?
- Are we *more* or *less* secure than our peers?
- Which are our strongest and weakest security points?
- What are our biggest security threats or concerns?
- Are we spending (investing) too much or too little on information security, or do we have it about right?
- Are our security resources allocated optimally?
- Have we properly and adequately treated all reasonably foreseeable information security risks?
- Can we handle compromises, breaches, and other information security incidents effectively and efficiently?
- Are we (sufficiently) compliant?
- Are we *best in class*? Are we perhaps overdoing it, or are we lagging the field in information security?

They point out that metrics can help improve information security systematically: "It could be argued that we have gotten where we are today mostly through a process of trial and error, hit or miss.... If we don't even track and record incidents properly and can barely guess at which incidents are costing us the most each month or year, how can we determine which changes are truly worth making?"

Their sound arguments in Chapter 2 are consistent with the point of view expressed a decade ago in an article I called "Net Present Value of Information Security." <a href="http://www.mekabay.com/infosecmgmt/npvsec.pdf">http://www.mekabay.com/infosecmgmt/npvsec.pdf</a> >

Chapter 6, "Metametrics and the PRAGMATIC approach" is at the core of their method. Their PRAGMATIC metametric framework stands for these elements in judging the usefulness of metrics:

- Predictive
- Relevant
- Actionable
- Genuine
- Meaningful
- Accurate

- Timely
- Independent
- Cheap.

The authors describe a practical series of steps for evaluating metrics systematically using these objectives and include many useful tips and case studies to help the practitioner.

Chapter 7 provides a detailed application of the PRAGMATIC approach using the ISO/IEC 27002:2005< <a href="http://www.iso.org/iso/catalogue\_detail?csnumber=50297">http://www.iso.org/iso/catalogue\_detail?csnumber=50297</a> > standards for information-security management. In this example, they apply their method to "metrics measuring the processes or outcomes typically used to indicate, assess, and address information security."

Just like the approach of Computer-Aided Thematic Analysis<sup>TM</sup><

<a href="http://www.mekabay.com/methodology/CATA.pdf">http://www.mekabay.com/methodology/CATA.pdf</a> and Computer-Aided Consensus<sup>TM</sup>,<

<a href="http://www.mekabay.com/methodology/cac.pdf">http://www.mekabay.com/methodology/cac.pdf</a> the PRAGMATIC analysis serves as a

<a href="http://www.mekabay.com/methodology/cac.pdf">heuristic</a> to encourage thoughtful analysis, discussion, and development. The specific scores assigned to each component of each particular metric cannot be defined completely objectively, but thinking about them and coming to agreement are enormously useful steps in developing a rational information-assurance strategy.

Chapter 8 focuses on this question: "...[H]ow, exactly, do we establish performance measures that will derive maximum value from information security?" Using a lifecycle approach rooted in decades of experience with spiral development methodology< <a href="http://www.ianswer4u.com/2011/12/spiral-model-advantages-and.html">http://www.ianswer4u.com/2011/12/spiral-model-advantages-and.html</a> > for systems, the authors step the readers through a cycle of stages leading to actionable metrics and preparing for the next round of improvement.

Chapter 9, "Advanced Information Security Metrics," explores lessons learned from other applications of metrics and specifically addresses the concepts and terminology for evaluating metrics, including

- High reliability
- Indicators and proxies
  - Key goal indicators
  - Key performance indicators
  - Key risk indicators
- Targets, hurdles, yardsticks, goals, objectives, benchmarks and triggers

Chapter 10, "Downsides of Metrics," takes a realistic view of what we can achieve with metrics, even the best of metrics. "...[T]here are inherent unpredictabilities with some information security metrics. We can do our level best to minimize them by using better, more reliable instrumentation and to smooth them out using ... statistical techniques ..., but they inevitably remain."

Chapter 11, "Using PRAGMATIC Metrics in Practice," looks in detail at sources of data, methods for analysis, data presentation, and responding to metrics.

Chapter 12 is a 40-page case study with real data anonymized for the canonical *Acme* 

*Enterprises*, *Inc*. It provides detailed commentary to help the reader apply these methods to the real world.

Chapter 13 provides parting thoughts on applying these methods with strong, useful recommendations for putting the PRAGMATIC metrics into practice.

I strongly recommend this text to all information-assurance practitioners; I think it can also be useful as a textbook in graduate degrees in the management of information assurance for a specific module on metrics and optimization of security strategy.

\* \* \*

For the record, I have no financial or professional relationship with the authors and the publisher of their text. They're just really smart and very nice folks.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2013 M. E. Kabay. All rights reserved.

## **Moving Forward on Backups**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

This week in the IS342 *Management of Information Assurance* course<
http://www.mekabay.com/courses/academic/norwich/is342/index.htm > at Norwich University<
http://programs.norwich.edu/business/csia/ >, my students and I have been discussing backups.
As part of my usual continuous process improvement, I've updated my lecture notes<
http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/index.htm > (which we no longer use in class, preferring to watch lectures from respected industry or academic experts and have vigorous discussions). The topic corresponds to Chapter 57<
http://www.mekabay.com/courses/academic/norwich/is342/is342\_lectures/csh5\_ch57\_backups.pptx > in the *Computer Security Handbook*, 5<sup>th</sup> Edition.< http://www.amazon.com/Computer-Security-Handbook-Volume-Set/dp/0471716529/ >

The biggest changes for choosing appropriate backup strategies since the 2009 publication of the 5<sup>th</sup> Edition are in

- The capacity and costs of backup media
- Transfer speeds
- The growing popularity of cloud backup.

I started the class discussion with a plea to my students to back up their work: I absolutely *hate* having to redo something I've already finished, and I asked if they would agree that trying to reconstitute work after we've already done it is much harder than one might expect. Especially in writing, we naturally suppress repetition – and as we rewrite our lost manuscript, we're constantly fighting the legitimate sense that we've already dealt with each topic. It's bad enough to have the dog eat our homework: having a dead or lost disk drive eat our homework should be much more embarrassing.

Luckily, the price of storage in many media has been dropping steadily for years. For example, a 3 TB magnetic disk drive currently costs around U\$120 – about U\$40/TB or \$0.000038/MB. When I started work with Hewlett Packard in 1980, our biggest disk drive (the HP7925 with 120 MB) cost U\$25,000 – around U\$100,000 in today's currency. That's about \$833/MB. Out of curiosity, I computed the annual change in price over 33 years (33<sup>rd</sup> root of today's price divided by the old price): it's about 0.6 per year. In other words, the price has dropped to 60% of the previous year's price every year for 33 years! I guess Moore's Law< <a href="http://www.mooreslaw.org/">http://www.mooreslaw.org/</a> > is still in force even for storage costs.

Transfer speeds are steadily rising, too. In 1980, we were happy with a seek time of around 25ms (millseconds) and a transfer rate of ~7 Kbps(kilobits per second)<
http://www.hpmuseum.net/document.php?hwfile=2686 >; today's *cheap* disk drives typically provide seek times in the millisecond range and data transfer rates in the Gbps range.

These changes are allowing us to increase the frequency and extent of our backups for fixed costs or to lower costs for existing backup patterns.

Another change is the availability of cloud backups<

http://www.thetop10bestonlinebackup.com/cloud-backup >, which allows users and organizations to store backups at a distance using Internet communications. Some of the services are free and many user-level services are relatively inexpensive. By configuring client software – or even just using a Web browser – users can store, update and retrieve their data from any of their computers from any of the locations that have 'Net access.

A useful guide called "Why Cloud Backup: Top 10 Reasons" < <a href="http://www.ironmountain.com/arma/docs/top\_ten\_reasons.pdf">http://www.ironmountain.com/arma/docs/top\_ten\_reasons.pdf</a> > from Iron Mountain < <a href="http://www.ironmountain.com/">http://www.ironmountain.com/</a> > discusses, well, 10 reasons for considering cloud backup:

- 1. Achieve disaster recovery with secure offsite cloud backup
- 2. Freedom from manual and complex tape backup tasks
- 3. Predictable costs for simpler budgeting
- 4. Reliable and guaranteed data recovery
- 5. Minimized risks and costs of downtime
- 6. Fast data restores
- 7. Take advantage of service provider's expertise and resources
- 8. Offload regulatory compliance requirements to service provider
- 9. Well-managed cloud more secure than your own
- 10. Ease of setup and use, set-and-forget, no training required.

Some of the concerns< <a href="http://www.zdnet.com/despite-risk-more-smbs-consider-cloud-backup-7000012745/">http://www.zdnet.com/despite-risk-more-smbs-consider-cloud-backup-7000012745/</a> about cloud backups are confidentiality of unencrypted data stored on someone else's system, the risks of having files inadvertently or deliberately deleted when cloud folders are shared with colleagues or friends, and the critical bottleneck of network bandwidth: regardless of how fast the cloud servers are working, the rate-limiting factor is usually the user's available bandwidth.

The rest of the class notes continue with the usual discussion of issues in backing up, such as storage and disposal of backups, extended costs (e.g., media, time, storage, maintenance), and questions of types and frequency of backups. Feel free to have a look!

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2013 M. E. Kabay. All rights reserved.

## **HIPAAcratic Oath**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

In the United States, the Health Insurance Portability and Accountability Act (HIPAA) < <a href="http://www.hhs.gov/ocr/privacy/">http://www.hhs.gov/ocr/privacy/</a> > governs security for personally identifiable health-related information; HIPAA determines which health-related information may be released and transferred to whom and how such information must be protected against unauthorized access, modification and destruction.

In the European Economic Community, the European Privacy Directive<
<a href="http://ec.europa.eu/justice/data-protection/">http://ec.europa.eu/justice/data-protection/</a> > and related agreements<
<a href="http://ec.europa.eu/justice/data-protection/document/national-policy/health-data/index\_en.htm">http://ec.europa.eu/justice/data-protection/document/national-policy/health-data/index\_en.htm</a> > provide rights for data subjects (sometimes differing from country to country) to access and control information about themselves, including health-related data.

Recently I realized that such laws have unintended consequences given the widespread availability of anonymous ratings of doctors on such services as Angies's List<a href="http://reviews.angieslist.com/wellness/doctor.aspx">http://reviews.angieslist.com/wellness/doctor.aspx</a> >, iDashboards.com<a href="http://www.idashboards.com/Solutions/For-Your-Industry/Healthcare.aspx">http://www.idashboards.com/Solutions/For-Your-Industry/Healthcare.aspx</a> >, and RateMDs<a href="http://www.ratemds.com/">http://www.ratemds.com/</a> > (among many others).

My wife (light of my life) is Dr Deborah N. Black, MDCM, CPSQ, FRCP(C)<
<a href="http://www.cvmc.org/news/2011-hire-deborah-black">http://www.cvmc.org/news/2011-hire-deborah-black</a> She's a brilliant neuropsychiatrist (she helps patients and psychiatrists diagnose and treat behavioural disorders that may be related to organic brain disease or trauma) who has over 30 years of experience in her field. She is *almost* universally adored by her patients, her staff and her colleagues; every time I visit her main office at the Central Vermont Medical Center< <a href="http://www.cvmc.org/">http://www.cvmc.org/</a> , the moment someone finds out that I'm her husband, I get showered with praise for her.

Here's the problem: a couple of weeks ago, Deborah saw a patient with a variety of complaints – and promptly received a bunch of complaints about Deborah's responses! The patient was angry about everything: how he was received by the receptionists, how Deborah articulated the medical problems, and the results of the tests he had taken under the doctor's supervision. The irony was that every single complaint was ill-founded: he accused Deborah of writing things that had not, in fact, been written into the record and misinterpreted the meaning of specific tests despite Deborah's repeated attempts to correct his misunderstanding. For example, the patient was furious about the results of a particular test which he insisted on misinterpreting as an IQ (intelligence quotient) test and raging that an IQ of 50 was impossible for him. It was nothing of the sort, but nothing Deborah said changed his determination to be insulted by the "low IQ" result.

The angry patient left the office in a rage, with threats of posting comments about Deborah's "unprofessional" behaviour – which, as we say in Vermont, made Deborah "wicked mad" because some years ago, someone posted an inflammatory list of accusations, all of which were false, on an anonymous professionals' evaluation service on the Web. When Deborah contacted the organization responsible for the list, she was firmly informed that there was no way she could

have the insulting, defamatory comments removed without a court order.

So here's the dilemma for all professionals who abide by standards of protecting personally-identifiable information. If they ignore libellous postings, their reputation may be harmed. If they attempt to challenge the false information using actual details of a patient's history or even behaviour during office or clinic visits, they will assuredly violate privacy-protection laws.

My colleague Professor David Blythe, JD pointed out in discussions of this issue that during a civil action for defamation, the professional suing for elimination of the libellous postings or for damages could challenge the factual basis of the allegedly libellous material – and not be bound by the strictures of data protection during the legal proceedings. For US attorneys, lawyer-client privilege allows the *client* to control what information about their communications with their lawyer may be made public – but there is a specific provision in the rules of evidence to allow an attorney accused of malpractice to defend herself even if that defence compromises client confidentiality: "Exceptions: There is no privilege under this rule: .... As to a communication relevant to an issue of breach of duty by the lawyer to his client or by the client to his lawyer...." [Legislative Council of the General Assembly for the State of Vermont (2003). *Vermont Rules of Criminal Procedures and Vermont Rules of Evidence*. LexisNexis (ISBN 0-327-04424-1) §502(d), p383].

Another issue he pointed out is that by beginning legal proceedings, the victim of libel may inadvertently give wider visibility to the libel.

But doctors, in particular, are bound not only by legal regulations: they also adhere by tradition to the Hippocratic Oath< <a href="http://www.pbs.org/wgbh/nova/body/hippocratic-oath-today.html">http://www.pbs.org/wgbh/nova/body/hippocratic-oath-today.html</a> often rendered as "First, do no harm." Fighting back against libel perpetrated by a mentally ill patient could be construed as doing harm – and my wife is unwilling to go that route.

Quite a bind, eh?

I think that there are strong reasons for providing the protective umbrella of anonymity and pseudonymity< <a href="http://www.mekabay.com/overviews/anonpseudo.pdf">http://www.mekabay.com/overviews/anonpseudo.pdf</a> when the victims of despotic regimes and other criminal organizations want to mobilize public opinion for action against injustice. I am not convinced that it is in the public interest to encourage anonymous postings that vilify professionals who cannot, due to their professional standards, defend themselves with factual information to counter the libel.

I welcome commentary on this complex issue.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

# **Data Destruction**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University

One of the problems in calling a professor for a quick insight into something they teach is that it's hard to shut us up.

Recently a very nice reporter called me for comments about data destruction; later I wondered if she was appalled by the length of the interview.

I think that one of the essential steps in planning for data destruction is to have a complete and up-to-date inventory of the life-cycles of all the types of information held by an organization. The information we need is likely to be found in service-level agreements, backup policies, business-continuity and disaster recovery plans. We have to know how long each type of data should be kept, and for what reasons. Important factors in such decisions are legal and regulatory requirements. Over a decade ago, I wrote,

Before engaging in any new data destruction, ...[we]... would do well to consult corporate counsel to establish the legal requirements that contribute to determining appropriate data retention policies. Different classes of data will have different retention periods mandated by law, regulations, or business requirements such as due diligence investigations preceding mergers and acquisitions.<
http://www.mekabay.com/nwss/133\_data\_destruction.pdf>

A primary concern among commercial organizations is that excessively long persistence of data increases the risk of expensive efforts to comply with court orders such as warrants and subpoenas. Having to search or even transfer orders of magnitude more data than necessary can be expensive in time and materials. In addition, old data fragments or repositories may no longer have the information to provide context for accurate interpretation of the old records. References which might explain apparently compromising memoranda may be missing, with dire results in court proceedings.

Another paragraph from that old article reads,

Any change in policies on data destruction should be closely coordinated with the information technology group to be sure that backups and archives are included in the analysis. Electronic or optical archives of documents, including e-mail -- and including backups -- are a rich source of data mining during the legal discovery process. In addition, your client should examine the distribution of documents it wishes to destroy but which reside on employees' desktop, laptop or even personal home computers. Unfortunately, many users have no idea that copying company information onto their home computers poses a security risk; in addition, many novices store documents higgledy-piggledy in a single folder (e.g., "My Documents") with no subfolders, with filenames such as "Document.doc" and with empty property sheets that convey nothing about the subject matter or provenance of the documents. Finding and extirpating all copies of documents that ought to be destroyed may be much harder than it seems at first

glance.

Data destruction policies cannot succeed without data-loss prevention policies and appropriate controls to ensure that employees follow acceptable standards for extraction and storage of data from corporate sources. For one thing, copies of data downloaded from active data sources become out-dated; employees who, for example, extract customer data from a master database may find that their information is out of date within days or weeks – and that decisions or calculations based on the old data may lead to errors.

In today's bring-your-own-device (BYOD) environment, strict policies on data retention become increasingly important; we don't want a statement to the court about the destruction of specific data to be contradicted by forensic examination of employee-owned devices.

Another implication of data-destruction policies is that no data must be destroyed without justification – and in particular, no data must be destroyed when there is a court order in place or even expected in the immediate future. Data cannot be destroyed capriciously; selective deletion of specific email threads, for example, could be construed as evidence of attempting to conceal malfeasance.

As for the methods of data destruction on storage media, professional services (look up "data destruction" in a search engine) are an excellent choice for small to medium businesses. These firms can provide securely locked receptacles for paper, for discarded magnetic media, for optical media and even for hard disk drives. On a regular schedule, they can either pick up the discards for treatment at a central facility or destroy the media on the spot using large-scale shredders.

Speaking of shredders, if readers need to buy small- or medium-scale shredders for their homes or offices, they should be sure to buy *cross-cut* shredders that fragment media into little diamond-shaped pieces. Old-style parallel-blade shredders produce paper that can be pieced together too easily for comfort. One recent example of poor shredding was the discovery in late November 2012 at the Macy's Thanksgiving Parade in Manhattan that some of the confetti thrown around at the celebration contained confidential – and readable – information from files of the Nassau County Police Department.< <a href="http://newsfeed.time.com/2012/11/27/macys-thanksgiving-day-parade-confetti-made-using-confidential-police-documents/">http://newsfeed.time.com/2012/11/27/macys-thanksgiving-day-parade-confetti-made-using-confidential-police-documents/</a>>

\* \* \*

A useful document from the US National Institute of Standards and Technology (NIST) that includes discussions of email retention policies is "NIST Special Publication 800-45, Version 2, "Guidelines on Electronic Mail Security" (February 2007). <

For more information about media sanitization standards, see Draft NIST Special Publication 800-88, Revision 1: "Guidelines for Media Sanitization" (September 2012).<a href="http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800\_88\_r1\_draft.pdf">http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800\_88\_r1\_draft.pdf</a>

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

# **Dropping the Ball on Dropbox**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Last week I nearly caused myself a heart attack when I thought I was backing up my Dropbox shared folders: all the files disappeared!

I use Dropbox< <a href="https://www.dropbox.com/">https://www.dropbox.com/</a> > to share files with students on student research projects and with colleagues to share course materials when we collaborate in teaching. For other projects, we use Google Drive< <a href="https://drive.google.com/">https://drive.google.com/</a> >. Similar functions are available on our university network through shared disk drives and SharePoint<<a href="http://office.microsoft.com/en-us/microsoft-sharepoint-collaboration-software-FX103479517.aspx?fromAR=3">http://office.microsoft.com/en-us/microsoft-sharepoint-collaboration-software-FX103479517.aspx?fromAR=3</a> >.

Because any change in a shared folder affects everyone depending on the shared resource, accidents can have serious consequences. For example, one of the folders I wiped out of our Dropbox was where my colleagues and I share all the current versions of chapters destined for a new edition of a reference book that has over 80 contributors. Another was where I store all the homework and exam materials for my statistics course – hundreds of hours in development time on the textbook, the homework, and the exams.

Luckily, the disappearance of all the Dropbox files was minor: it turns out that I accidentally backed up everything to the same hard drive as the Dropbox folder – so I actually *moved* instead of *copying* the files. It took less than a minute to move the 2.32 GB back into the right folder; however, it took significantly longer to update the remote drives at Dropbox with the files – and then update the other users' hard-disk versions – because of bandwidth limitations.

The incident has reinforced my belief that taking independent backups of such shared resources is essential. My daily routine includes launching backup processes that generate dated differential backups (backing everything up since the last backup), including backups of the Dropbox.

Differential backups are fine, but recovering from a real disaster would require restoring all the data from the latest full backup and then updating from each differential backup. Unfortunately, that process puts deleted files back in place and one must delete unwanted files manually.

Lately I have switched to taking full dated backups of the Dropbox every day. Recovering from an accident consists simply in restoring everything from that full backup.

When there are multiple users, the likelihood of a problem increases exponentially – that is, as a function of the number of users, n.

For any shared resources where all participants have the ability to add, change or delete content, we should remember how to calculate the likelihood of a problem when n different users are involved:

- Let the probability of a failure caused by user (i) be p(i)
- Then the probability of not having a failure caused by user (i) is [1 p(i)]

- And the probability that all the n users will cause no failure is  $[1 p(1)]*[1 p(2)]*[1 p(3)]* \dots [1 p(n)]$
- For simplicity in this example, let p(i) = p for all n users
- Thus the probability that there will be no failure is simply  $P\{\text{no errors}\} = (1-p)^n$
- So the probability that at least 1 user will cause a failure is  $P\{\text{at least one error}\} = 1 (1 p)^n$

If the chance that a user will make a mistake in the shared files is, say 0.01 per year and there are 10 users, then

```
P{at least one error} = 1 - (1 - 0.01)^10 = 1 - 0.99^10 = 1 - 0.904 = 0.096.
That is, there is a roughly 1 in 10 chance that someone in the group will cause an error in the next year.
```

Change the number of users to 100 and the picture is much more alarming:  $P\{\text{at least one error}\} = 1 - 0.99^100 = 1 - 0.366 = 0.634 \text{ or roughly 2 in 3.}$ 

Up the number of participants another order of magnitude to 1,000 users and we have  $P\{\text{at least one error}\} = 1 - 0.99^1000 = 1 - 4.3e-05 \approx 1.$ 

In conclusion, I think it is essential that any group sharing files determine who shall take *daily* backups of the materials. As long as there is a system for backing up and the backups are safely stored, it should be possible to recover from accidental (or deliberate) damage.

On a related note, agreeing on file-naming conventions is essential for effective collaboration. My practice is to save files with incremented version numbers (e.g., text\_v08.docx is saved as text\_v09.docx) when I finish working on a document. For convenience, I also save the file immediately without the version number (text.docx) so that it represents the latest version and I can pin that filename to the list of recent files for quick access. However, if there are several people editing a file, I strongly recommend that the group agree on using TRACK CHANGES so that it's clear who did what.

If there are many people working simultaneously, problems will arise due to the same problems that occurred in early versions of databases. The *lost update* problem occurs when uncontrolled access to a file allows Albert to open text.docx and then moments later, Bob to do the same. Each merrily updates the file; if Albert saves it first, then when Bob saves to the same filename, Bob's changes will destroy the record of Albert's changes.

Databases control such problems by providing locking strategies. If our shared folder doesn't allow that, one easy solution (although it requires everyone to use it reliably) is to define a folder such as "in use" and move the original file there so no one else uses it. In the shared folders for the new edition of the book I mentioned above, our team uses suffixes for the name of the chapter; e.g., "ch45" is not currently being updated; "ch45\_au" is being modified by the author(s); "ch45\_ed" is being edited; "ch45\_pub" has been sent to the publisher.

Happy collaboration!

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

# **Beyond Technical Security: Three Principles for Life**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

On Wednesday the 24<sup>th</sup> of April 2013, the School of Business and Management<
<a href="http://programs.norwich.edu/business/">http://programs.norwich.edu/business/</a> > at Norwich University celebrated the induction of a dozen students into the computing honour society Upsilon Pi Epsilon < <a href="http://upe.acm.org/">http://upe.acm.org/</a> > and of the business and management students into Delta Mu Delta < <a href="http://deltamudelta.org/">http://deltamudelta.org/</a> >.

We had a splendid supper and pleasant conversation, and then our Director Dr Najiba Benabess < <a href="http://www.linkedin.com/pub/najiba-benabess/38/277/531">http://www.linkedin.com/pub/najiba-benabess/38/277/531</a> > led us through the evening's celebrations.

When everything was finished, Dr Benabess and I played a trick on our captive audience. She introduced me as the last speaker of the evening, and by arrangement, turned to me and said severely, "Now remember, Prof Kabay, no more than 40 minutes!" I looked pained and complained that I didn't see how I could fit all my advice into only 40 minutes. I told the students and faculty that I'd try to fit everything in, but that I had a great deal to give them and they should loosen their belts and get relaxed, because this would take considerable time.

By this point, most of the people in the audience were looking at their watches and looking downcast at the prospect of yet another speaker – especially one complaining of having only 40 minutes.

My actual speech took about 90 seconds and made three points. I've expanded my comments to take advantage of this written format.

1. **Question Authority.** Don't ever let social or professional status get in your way of thinking critically and sceptically. If something you're being told or told to do doesn't make sense, ask questions (politely) until it does – or until you and your interlocutor understand that the initial instructions or statements were wrong or need clarification. If you don't understand what an expert is saying, say so: ask for clarification. You don't have to interrupt a public lecture – be sensitive to context – but you shouldn't let the issue slide.

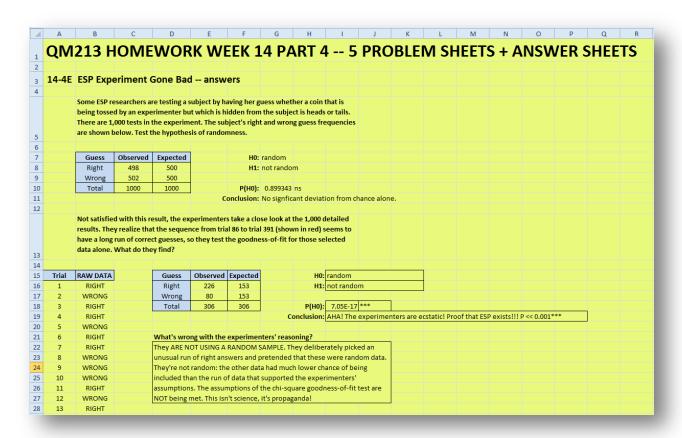
My favourite story about questioning authority is from the 1980s when I taught at John Abbott College< <a href="http://www.johnabbott.qc.ca/welcome">http://www.johnabbott.qc.ca/welcome</a> > in the west end of Montreal Island<

http://ville.montreal.qc.ca/portal/page?\_pageid=5977,86481579&\_dad=portal&\_schema=PO RTAL >. I took my database students (from the John Abbott Programmers Course, JPC) to Place Ville Marie< http://www.placevillemarie.com/en/home.php > for a lecture by a major vendor about their newest database software. There were about 300 professionals in the audience. Partway through the lecture, the speaker said something like, "And we used the matrix-analytical method to optimize the design." I put up my hand. "Yes?" said the speaker. "I'm sorry," I said apologetically, "but I don't know what the matrix-analytical method is." The speaker stared at me in horror for a moment. He burst out, "Neither do I!" Turned out he

was using someone else's notes. The audience roared and my students were impressed with the sincerity of my instructions to them about asking for explanations without embarrassment. Twenty years later, I got an email from one of my old JPC students reminding me of the incident and saying that it had stayed with him all these years.

2. **Reality Trumps Theory.** No matter what the textbooks say, no matter what's in the journals, and no matter what the experts say, focus on the actual situation you are facing. Don't let generalities and customary assumptions block you from seeing the real-world details of the problem you are trying to solve.

In my statistics classes this week, I've been showing students some classic errors of the application of statistical methods. Here's a screenshot of one of the exercises in goodness-of-fit calculations:



In class, I pointed out that selection bias< <a href="http://skepdic.com/selectionbias.html">http://skepdic.com/selectionbias.html</a> > can ruin the validity of statistical analysis. For example, if an unsophisticated, uneducated grocery clerk is instructed by his boss to show that their oranges are bigger than their competitor's oranges, the poor clerk may deliberately or perhaps unconsciously select the biggest oranges in his employer's bins and the smallest oranges in the competitor's bins. Any attempt to conclude something like "The probability that the observed chi-square value or larger could">http://skepdic.com/selectionbias.html</a> > can ruin the validity of statistical analysis. For example, if an unsophisticated, uneducated grocery clerk is instructed by his boss to show that their oranges are bigger than their competitor's oranges in his employer's bins and the smallest oranges in the competitor's bins. Any attempt to

occur by chance alone if the null hypothesis of equal orange sizes were true is only 10^-17" fails on the issue of "by chance alone."

On a related note, readers may like the lecture on "How to Solve Technical Problems" < <a href="http://www.mekabay.com/courses/academic/jac/TSP/2\_prob.ppt">http://www.mekabay.com/courses/academic/jac/TSP/2\_prob.ppt</a> > from my old JPC course on The Art of Technical Support<

<u>http://www.mekabay.com/courses/academic/jac/TSP/index.htm</u> >. Some of the principles articulated in that course are

- Get the global picture
- Distinguish observation from assumption
- Distinguish observation from hearsay
- Distinguish observation from hypothesis
- Challenge your hypothesis.
- 3. **Better Crazy than Boring.** This has only a little to do with information security but a great deal to do with life in general. I believe that being unpredictable in one's thinking and behaviour is an excellent life habit. Refusing to allow oneself to fall into rigid patterns of thinking and behaviour can lead one to novel perceptions and creative solutions.

From a security standpoint, being unpredictable in one's monitoring and configurations deprives the attacker of a repeatable, predictable target. Uniformity may be helpful in many circumstances, but adapting to the particulars of a specific network or system can also be helpful.

Being a bit crazy can enliven our teaching, our professional lives, our marriages, and our lives in general. For example, when I teach, sometimes I change my accent to keep the students awake; I'll switch into Russian, Indian, French, German and various sorts of British accents to the amusement of my students – who then don't fall asleep due to their 05:00 physical training exercises (most of our students are in the Corps of Cadets<
http://www.norwich.edu/campus/together.html > at Norwich). As for my wife and I, we never know what the other is going to do or say. Just this week Deborah came home late while our dogs were away; since the two doggies routinely clamber into Deborah's car when she arrives, I did so instead to much laughter. After 30 years together, we still laugh with each other every day.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

# **Priorities**

## by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University

Northfield, Vermont< <a href="http://www.northfield-vt.gov/">http://www.northfield-vt.gov/</a> is a tiny village in the green hills of a beautiful state</a> <a href="http://vermont.gov/portal/">http://vermont.gov/portal/</a> > with a population of only about 620,000 people — the second smallest in the USA. With a population density of only 26 people per square kilometre, traffic jams are rare in the state. In Northfield, with only 6,000 residents and about 1,000 faculty and staff commuting to Norwich University<
a href="http://www.norwich.edu/about/nucampus.html">http://www.norwich.edu/about/nucampus.html</a> >, traffic jams are almost nonexistent. One of my colleagues joked a few years ago, "Well, things can get pretty tight during rush minute."

Construction has resumed in Northfield this week to repair the main road, which is showing potholes and deep cracks developed over several years of the winter-spring freeze-all cycles. When I drove down the major road leading to Northfield from Interstate 89 yesterday (May Day) at around 07:30, I was astonished to find a line-up of stationary cars over a mile in length. After 15 minutes of being stationary, I called the 911 emergency services on my mobile phone.

"911 – what is your emergency?"

"There is a brain-damaged person running the traffic control on Route 12 entering Northfield from the South."

"How do you know that this person is brain-damaged?"

"Because only a brain-damaged person would hold up several hundred cars to allow five – no, six, excuse me – cars to get by in the opposite direction."

The operator put me in touch with local police and a few minutes later I noticed the blue flashing lights of a police cruiser arriving and the traffic began to move again.

And so what does this have to do with security?

What struck me is that the person controlling the traffic was allocating equal priority to the 300 cars lined up trying to get into Northfield and the 10 cars waiting to get out of Northfield. There were also apparently giving priority to a small number of construction vehicles pottering about trying to get their work done. No one in the construction company team seemed to be aware of the costs they were imposing on a great many employees and students of the University: they were making a great many people late for their 08:00 classes. University regulations stipulate that students whose teacher fails to arrive by 10 minutes after the official start of class may leave without penalty.

Why would anyone in a construction company give a rat's rear end about delaying classes?

Just as in operations management, security in general, and business continuity planning in particular, anyone setting priorities has to consider the field of stakeholders. Stakeholders are

everyone affected by how we run our business; for example, a commercial organization would define stakeholders to include customers, employees, participants in the supply chain, and the wider community depending on or affected by the organizations activities. Examples of the latter could be businesses depending on the economic activity of the organizations employees; in communities around a major hospital, local businesses may depend on economic activities of patients and visitors to the hospital.

When the traffic controller used a rigid timing pattern that gave equal weight to the tiny number of cars leaving the little town as to the large number of cars trying to get to Norwich University, the consequences – costs – were far greater for the people in the huge line-up and for students who ended up missing the first classes of the day because their instructors were waiting for half a dozen people to get by several hundred waiting drivers.

In business continuity planning, one of the most important elements is a clear understanding of critical-path relationships among the many tasks that must be accomplished for continuity of operations. In the critical-path method (CPM< <a href="http://www.mindtools.com/critpath.html">http://www.mindtools.com/critpath.html</a> ), we identify dependencies and establish a timeline to ensure that all the prerequisites for every step are in place. Part of the reasoning for CPM is estimation of consequences of different degrees of delay. For example, in a company doing business via the Web, the accounting components that allow users to place orders and pay for their desired product or service immediately become of critical importance. If an online bookstore can't even take an order within a few seconds, it's quite possible for a prospective buyer simply to switch to a competitor within seconds. In such a case, continuity of operations must define the accounts-receivable functions as top priority. In contrast, the same company could define accounts-payable functions as lower priority because of the traditional 30-day period allowed for payment. In contrast, an engineering company working through extended, complex bids and contract-development period measured in months or longer might consider the accounts-receivable functions at the same level of relatively low priority in the business resumption plan as the accounts-payable functions.

Another example from my own consulting work (25 years ago!) is the case of a government agency whose night-time batch processing was taking longer and longer. It had once taken only a few hours; by the time I was called in, the batch processing was often overlapping with the start of the 07:00 shift – and several hundred unionized employees were unable to start their work on time.

So what? One might think that a few hours delay hardly warranted replacement of a multimillion-dollar computer system.

Oh yes it did.

The union contract required every employee to be allowed the same amount of time caused by the delay to be added to the end of their shift – at time-and-a-half rates. Thus the agency was paying for about 200 employees to wait around at full pay (around \$2,000 a day), unable to access the necessary computer services and then pay 150% of what they'd already paid for at the end of the day (another \$3,000 on top). You can understand that with costs of about \$5,000 a day (\$100,000 a month, \$1,200,000 a year) why the agency wanted to know if it was time for a new \$2.5M computer system.

That was the case in which I was able to write the shortest Executive Summary I've ever managed to present:

Question: Should the agency buy a new computer to speed night-time batch processing? Answer: No.

The next page was entitled "Slightly Less Executive Summary" and explained that there had been inadequate maintenance in some of the production databases; adding some indexes and recompacting some datasets brought the batch processing back to a completion point around 03:30 in the morning.

The construction firm (or specific employees) that allowed the relatively huge traffic jam to develop in our little town do not appear to have set priorities with which the major employer, Norwich University, would agree. In the long run, given the enormous influence of the University on the local economy of Northfield, a complaint from University authorities to the administrators in the town might have deleterious effects on future contracts with that particular construction company.

We shouldn't use easy, rigid rules (e.g., "Wait the same time for each direction of traffic") when setting our operational priorities. We need a clear evaluation of the immediate and long-term effects of the alternatives.

THINK.

\* \* \*

# **Updates to History of Computer Crime**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University

I've been updating chapters in the upcoming edition of a textbook and hope readers will find some of the research interesting. This week I'm posting materials I added to the chapter on the history of computer crime.

## **Late 2000s: Russian Business Network (RBN)**

The Russian Business Network (RBN) may have originated as a legitimate Web hosting company in 2006:

According to internet security company Verisign, which in June published an extensive investigation into the Russian outfit (tinyurl.com/ywvgpg), RBN was registered as an internet site in 2006.

Initially, much of its activity was legitimate. But apparently the founders soon discovered that it was more profitable to host illegitimate activities and started hiring its services to criminals. Verisign says simply that it is now "entirely illegal". Since then its activities have been monitored by a number of organisations, including the London-based anti-spam group Spamhaus. "RBN is among the world's worst spammer, child-pornography, malware, phishing and cybercrime hosting networks," says a spokesman. "It provides 'bulletproof' hosting, but is probably involved in the crime too." [1]

A researcher for the Internet Storm Center, "David Bizeul, spent the past three months researching the Russian Business Network (RBN). The RBN is a virtual safe house for Russian criminals responsible for malicious code attacks, phishing attacks, child pornography and other illicit operations...." Bizeul's study is a 70-page report with extensive documentation about the criminal activities of the RBN.[²] The group has supported malware diffusion, spam, phishing, denial of service, distribution of cyberattack tools, pornography and child pornography.

A 2011 report by David Goldman included the following useful insights:

"It's not like the Mafia, it is a Mafia running these operations," said Karim Hijazi, CEO of botnet monitoring company Unveillance. "The Russian Mafia are the most prolific cybercriminals in the world."

Organized cybercrime is a truly international affair, but the most advanced attacks tend to stem from Russia. The Russian mob is incredibly talented for a reason: After the Iron Curtain lifted in the 1990s, a number of ex-KGB cyberspies realized they could use their expert skills and training to make money off of the

hacked information they had previously been retrieving for government espionage purposes.

Former spies grouped together to form the Russian Business Network, a criminal enterprise that is capable of some truly scary attacks. It's just one of many organized cybercriminal organizations, but it's one of the oldest and the largest.

"The Russians have everyone nailed cold in terms of technical ability," said Greg Hoglund, CEO of cybersecurity company HBGary. "The Russian crime guys have a ridiculous toolkit. They're targeting end users in many cases, so they have to be sophisticated."[<sup>3</sup>]

## Anonymous

In 2003, political activists with a penchant for computer skills formed a loose association calling itself *Anonymous* for collaboration in a range of cyberattacks on targets its members disliked. The philosophy of the group explicitly rejects any centralized controls; anyone can claim to be a member of Anonymous.

In 2008, self-identified members of the movement labeling their efforts *Chanology*[<sup>4</sup>] attacked the Church of Scientology (readers interested in following the reference provided above should be aware that the site is loaded with pornographic advertisements for pornography sites). Members also harassed organizations attempting to strengthen intellectual property laws and enforcement or anti-piracy restrictions. Other targets of the non-organization include the Epilepsy Foundation, hip-hop Websites, Sarah Palin's political campaign, the government of Iran, the government of Australia, and the Tea Party chapter in Oregon.

One of the most publicized campaigns was in support of Julian Assange, leader of the WikiLeaks Foundation, whose group made public more than a million documents classified by the US and other governments as restricted or secret and revealing embarrassing details of several wars and internal communications among diplomats.

In January 2013, members announced that they would release large amounts of US government restricted information. They let the world know about their plans by posting their messages on a hacked US government Website.[5]

# **Unlimited Operations**

In May 2013, eight criminal hackers, New York City area members of a much larger worldwide ring of cybercriminals calling themselves Unlimited Operations were charged with theft of over \$45M from automated teller machines (ATMs) around the planet. The gang "used sophisticated intrusion techniques to hack into the systems of global financial institutions, steal prepaid debit card data, and eliminate withdrawal limits. The stolen card data was then disseminated worldwide and used in making fraudulent ATM withdrawals on a massive scale across the globe...."

In the first phase, the criminals broke into National Bank of Ras Al-Khaimah PSC (RAKBANK) in the United Arab Emirates. Using these compromised data, the criminal network completed over 4,500 ATM transactions in 20 and stole over \$5M.

The second phase began "...on the afternoon of February 19 and lasted into the early morning of February 20, 2013. This operation again breached the network of a credit card processor that serviced MasterCard prepaid debit cards, this time issued by the Bank of Muscat, located in Oman." Total losses from 36,000 transactions in 24 countries netted \$40 million in cash from ATMs.[6]

## **Industrial Espionage**

Why spend money developing competitive products when you can steal the work once it's ready to apply? Many firms in countries with little or no rule of law have taken advantage of poor security, outsourcing, and liberal immigration policies to steal intellectual property and compete at a discount with the originators of the ideas.

In 2001, Junsheng Wang of Bell Imaging Technologies pled guilty to violation of 18 USC 132(a)(2) by stealing trade secrets fom Acuson Corporation. The Counterintelligence News and Developments (CIND) report noted, "In pleading guilty, Wang admitted that prior to August 24, 2000, that he took without authorization and copied for Bell Imaging a document providing the architecture for the Sequoia ultrasound machine that contained the trade secrets of Acuson Corporation. According to Wang's plea agreement, he had been able to obtain access to the Acuson trade secret materials because his wife was employed as an engineer at that company and because she had brought that document into their home. After he had copied the document, he took it with him on business trips to the People's Republic of China, turning it over to Bell Imaging during 2000."[7]

In May 2001, Federal authorities arrested two Lucent scientists and a third man described as their business partner on May 4, charging them with stealing source code for software associated with Lucent's PathStar Access Server and sharing it with Datang Telecom Technology Co., a Beijing firm majority-owned by the Chinese government. The software is considered a "crown jewel" of the company. Chinese nationals Hai Lin and Kai Xu were regarded as "distinguished members" of Lucent's staff up until their arrests. The motivation for the theft, according to court documents, was to build a networking powerhouse akin to the "Cisco of China." The men faced charges of conspiracy to commit wire fraud, punishable by a maximum five years in prison and a \$250,000 fine.[8] In April 2002, the two were also charged with stealing secrets from four companies in addition to Lucent: Telenetworks, NetPlane Systems, Hughes Software Systems, and Ziatech. An additional Chinese national, Yong-Qing Cheng was also charged. They developed a joint venture with the Datang Telecom Technology Company of Beijing to sell a clone of Lucent's Path Star data and voice transmission system to Internet providers in China.[9]

In September 2002, the 3DGeo company in Mountain View, CA accused Shan Yanming, an employee of the China National Petroleum Corporation on loan to the company, of industrial espionage for trying to steal the software designed for using seismic data to map oil deposits. He was caught trying to download corporate data to his personal computer and ws arrested by FBI agents.[<sup>10</sup>]

In April 2003, the United States Attorney's Office for the Northern District of California announced that Tse Thow Sun pled guilty on April 9, 2003 to theft of trade secrets. He admitted that in early 2002, while working for a language translation company, he delivered a laptop computer and a hard drive that contained trade secrets and confidential proprietary information to a competitor and asked for \$3M in payment. Mr. Sun, 32, a citizen of Singapore, was indicted by a federal Grand Jury on April 9, 2002. He was charged with theft of trade secrets, in violation of 18 U.S.C. § 1832(a)(3); attempted theft of trade secrets, in violation of 18 U.S.C. § 2314. Under the plea agreement, Mr. Sun pled guilty to theft of trade secrets.[11]

In May 2003, three Swedish employees of LM Ericsson were charged with espionage for allegedly stealing intellectual property and sending it to Russian spies. "[Afshin] Bavand was arrested Nov. 5, 2002, while talking to a Russian intelligence agent in a Stockholm suburb. Police searched the Russian, who wasn't identified, and found \$4,000 in cash and Ericsson documents."[12]

The series of attacks codenamed *Titan Rain* was discovered by Shawn Carpenter in late 2003. Carpenter noticed a flood of expert hacker activity focusing on data theft from a wide range of "the country's most sensitive military bases, defense contractors and aerospace companies." Carpenter discovered that "the attacks emanated from just three Chinese routers that acted as the first connection point from a local network to the Internet." Carpenter worked with US Army and FBI investigators to learn more about the attacks and the attackers. According to Thornburgh, various analysts judge that "Titan Rain is thought to rank among the most pervasive cyberespionage threats that U.S. computer networks have ever faced."[13]

In July 2004, an Indian software engineer employed by a US company's software development center in India was accused of "zipping up" proprietary software source code for printing identification cards and uploading it to her personal e-mail account. Jolly Technologies shut down its Mumbai operations as a result of the breach of security.[14]

In 2005 and 2006, EMC filed lawsuits against several employees for allegedly stealing trade secrets. [15]

In December 2006, two Chinese nationals, Fei Ye and Ming Zhong, pleaded guilty in December 2006 to charges of economic espionage on behalf of the People's Republic of China. They were arrested in November 2001 with stolen trade secrets in their luggage; the information was taken from Sun Microsystems and Transmeta Corporation. The agents were planning to design a competing microprocessor using the stolen designs; profits were to have been shared with the City of Hangzhou and the Province of Zhejiang. The agents' company was funded in part by the National High Technology Research and Development Program of China.[<sup>16</sup>]

In April 2008, sleeper agent Chi Mak, a naturalized US citizen who lived peacefully in Los Angeles for 20 years, was sentenced to 24.5 years in federal prison for industrial espionage. He stole detailed plans for US Navy equipment including submarine propulsion systems and tried to send them to China via his brother and sister-in law.[17]

In 2009, Siobhan Gorman, writing in *The Wall Street Journal*, reported as follows:

Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national-security officials. The

spies came from China, Russia and other countries, these officials said, and were believed to be on a mission to navigate the U.S. electrical system and its controls. The intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war. "The Chinese have attempted to map our infrastructure, such as the electrical grid," said a senior intelligence official. "So have the Russians." The espionage appeared pervasive across the U.S. and doesn't target a particular company or region, said a former Department of Homeland Security official. "There are intrusions, and they are growing," the former official said, referring to electrical systems. "There were a lot last year."[18]

The Office of the National Counterintelligence Executive (ONCIX) published its *Report to Congress on Foreign Economic Collection and Industrial Espionage 2009-2011* with the title *Foreign Spies Stealing US Economic Secrets in Cyberspace*. The Executive Summary included this commentary:

"Sensitive US economic information and technology are targeted by the intelligence services, private sector companies, academic and research institutions, and citizens of dozens of countries.

Chinese actors are the world's most active and persistent perpetrators of economic espionage. US private sector firms and cybersecurity specialists have reported an onslaught of computer network intrusions that have originated in China, but the IC cannot confirm who was responsible.

Russia's intelligence services are conducting a range of activities to collect economic information and technology from US targets.

Some US allies and partners use their broad access to US institutions to acquire sensitive US economic and technology information, primarily through aggressive elicitation and other human intelligence (HUMINT) tactics. Some of these states have advanced cyber capabilities."[19]

A March 2012 report detailed how a successful supervisory control and data acquisition (SCADA) software company, American Superconductor Corporation (AMSC), was practically destroyed economically by its major customer, the Chinese Sinovel company, which stole its proprietary wind-turbine software and then stopped paying for any further software services.<sup>[20]</sup>

By early 2013, Symantec's 2012 Internet Security Threat Report, Vol, 18 reported that small businesses were increasingly targeted for cyber attacks and industrial espionage: "In 2012, 50 percent of all targeted attacks were aimed at businesses with fewer than 2,500 employees. In fact, the largest growth area for targeted attacks in 2012 was businesses with fewer than 250 employees; 31 percent of all attacks targeted them." [21]

\* \* \*

Copyright © 2013 M. E. Kabay. All rights reserved.

#### END NOTES FOR PUBLICATION

- [1] (Warren 2007)
- [2] (Bizuel 2007)
- [3] (Goldman 2011)
- [4] (Anonymous 2012)
- [5] (Ferenstein 2013)

- [6] (US Department of Justice 2013)
- [7] (San Francisco Business Times 2001)
- [8] (Backover 2001)
- [9] (New York Times 2002)
- [10] (Markoff 2002)
- [11] (US Department of Justice 2003)
- [12] (USA TODAY 2003)
- [13] (Thornburgh 2005)
- [14] (Ribeiro 2004)
- [15] (Wallack 2006)
- [16] (US Department of Justice 2006)
- [17] (Warrick and Johnson 2008)
- [18] (Gorman 2009)
- [19] (Office of the National Counterintelligence Executive (ONCIX) 2011)
- [20] (Riley and Vance 2012)
- [21] (Symantec 2013)

### REFERENCES FOR PUBLICATION

"Ms Smith". "DHS: Imported Tech Tainted with Backdoor Attack Tools." *NetworkWorld | Privacy and Security Fanatic*. 07 12, 2011. <a href="http://www.networkworld.com/community/blog/dhs-imported-tech-tainted-backdoor-attack-too">http://www.networkworld.com/community/blog/dhs-imported-tech-tainted-backdoor-attack-too</a> (accessed 05 16, 2013).

Anonymous. "Portal: Anonymous/Chanology." *Encyclopedia Dramatica*. 10 29, 2012. <a href="https://encyclopediadramatica.se/Portal:Anonymous/Chanology">https://encyclopediadramatica.se/Portal:Anonymous/Chanology</a> (accessed 05 16, 2013).

Backover, Andrew. "Feds: Trio stole Lucent's trade secrets." *USA TODAY*. 05 03, 2001. <a href="http://usatoday30.usatoday.com/life/cyber/tech/2001-05-03-lucent-scientists-china.htm">http://usatoday30.usatoday.com/life/cyber/tech/2001-05-03-lucent-scientists-china.htm</a> (accessed 05 16, 2013).

Bizuel, David. "Russian Business Network study." bizuel.org. 11 20, 2007. http://www.bizeul.org/files/RBN\_study.pdf (accessed 05 16, 2013).

Ferenstein, Gregory. "Anonymous Threatens Massive WikiLeaks-Style Exposure, Announced On Hacked Gov Site." *TechCrunch*. 01 26, 2013. <a href="http://techcrunch.com/2013/01/26/anonymous-threatens-massive-wikileaks-style-exposure-announced-on-hacked-gov-site/">http://techcrunch.com/2013/01/26/anonymous-threatens-massive-wikileaks-style-exposure-announced-on-hacked-gov-site/</a> (accessed 05 16, 2013).

Finkle, Jim. "Researchers say Stuxnet was deployed against Iran in 2007." *Reuters*. 02 26, 2013. <a href="http://www.reuters.com/article/2013/02/26/us-cyberwar-stuxnet-idUSBRE91P0PP20130226">http://www.reuters.com/article/2013/02/26/us-cyberwar-stuxnet-idUSBRE91P0PP20130226</a> (accessed 05 16, 2013).

Goldman, David. "The cyber Mafia has already hacked you." *CNNMoney*. 07 07, 2011. <a href="http://money.cnn.com/2011/07/27/technology/organized\_cybercrime/index.htm">http://money.cnn.com/2011/07/27/technology/organized\_cybercrime/index.htm</a> (accessed 05 16, 2013).

Gorman, Siobhan. "Electricity Grid in U.S. Penetrated By Spies." *Wall Street Journal*. 04 08, 2009. <a href="http://online.wsj.com/article/SB123914805204099085.html">http://online.wsj.com/article/SB123914805204099085.html</a> (accessed 05 16, 2013).

Javelin Strategy & Research. "2013 IDENTITY FRAUD REPORT: Data Breaches Becoming a

Treasure Trove for Fraudsters." Javelin. 2013. <a href="https://www.javelinstrategy.com/brochure/276">https://www.javelinstrategy.com/brochure/276</a> (accessed 05 16, 2013).

Langton, Lynn. "Identity Theft Reported by Households, 2005-2010." *Bureau of Justice Statistics*. 11 30, 2011. <a href="http://www.bjs.gov/index.cfm?ty=pbdetail&iid=2207">http://www.bjs.gov/index.cfm?ty=pbdetail&iid=2207</a> (accessed 05 16, 2013).

Markoff, John. "Silicon Valley Concern Says It Thwarted Software Theft." *New York Times*. 09 20, 2002. <a href="http://www.nytimes.com/2002/09/20/technology/20SOFT.html">http://www.nytimes.com/2002/09/20/technology/20SOFT.html</a> (accessed 05 16, 2013).

*New York Times*. "Trade-Secret Case Is Expanded." *New York Times*. 04 12, 2002. http://www.nytimes.com/2002/04/12/technology/12LUCE.html (accessed 05 16, 2013).

Office of the National Counterintelligence Executive (ONCIX). "Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-1011." Office of the National Counterintelligence Executive. 11 03, 2011.

http://www.ncix.gov/publications/reports/fecie\_all/Foreign\_Economic\_Collection\_2011.pdf (accessed 05 16, 2013).

Ribeiro, John. "Source code stolen from U.S. software company in India: Jolly Technologies blamed an insider for the theft." *Computerworld*. 08 05, 2004. <a href="http://www.computerworld.com/s/article/95045/Source\_code\_stolen\_from\_U.S.\_software\_company\_in\_India?taxonomyId=082">http://www.computerworld.com/s/article/95045/Source\_code\_stolen\_from\_U.S.\_software\_company\_in\_India?taxonomyId=082</a> (accessed 05 16, 2013).

Riley, Michael, and Ashlee Vance. "Inside the Chinese Boom in Corporate Espionage." *Bloomberg Businessweek*. 03 15, 2012. <a href="http://www.businessweek.com/articles/2012-03-14/inside-the-chinese-boom-in-corporate-espionage">http://www.businessweek.com/articles/2012-03-14/inside-the-chinese-boom-in-corporate-espionage</a> (accessed 05 16, 2013).

San Francisco Business Times. "Guilty pleas in trade secret case." San Francisco Business Times. 04 27, 2001. <a href="http://www.bizjournals.com/eastbay/stories/2001/04/23/daily42.html">http://www.bizjournals.com/eastbay/stories/2001/04/23/daily42.html</a> (accessed 05 16, 2013).

Symantec. "Internet Security Threat Report 2013." Symantec. 04 15, 2013. <a href="http://www.symantec.com/content/en/us/enterprise/other\_resources/bistr\_main\_report\_v18\_2012\_21291018.en-us.pdf">http://www.symantec.com/content/en/us/enterprise/other\_resources/bistr\_main\_report\_v18\_2012\_21291018.en-us.pdf</a> (accessed 05 16, 2013).

Thornburgh, Nathan. "Inside the Chinese Hack Attack." *TIME*. 08 25, 2005. http://www.time.com/time/nation/article/0,8599,1098371,00.html (accessed 05 16, 2013).

US Department of Justice. "Chicago, Illinois Man Pleads Guilty to Theft of Trade Secrets, Offered to Sell Online Interpreter's Information." US Department of Justice | Northern District of California. 04 11, 2003. <a href="http://www.justice.gov/criminal/cybercrime/press-releases/2003/sunPlea.htm">http://www.justice.gov/criminal/cybercrime/press-releases/2003/sunPlea.htm</a> (accessed 05 16, 2013).

- —. "Eight Members of New York Cell of Cybercrime Organization Indicted in \$45 Million Cybercrime Campaign." US Department of Justice | Eastern District of New York. 05 09, 2013. <a href="http://www.justice.gov/usao/nye/pr/2013/2013may09.html">http://www.justice.gov/usao/nye/pr/2013/2013may09.html</a> (accessed 05 16, 2013).
- —. "Two Men Plead Guilty to Stealing Trade Secrets from Silicon Valley Companies to Benefit

China." US Department of Justice | Northern District of California. 12 14, 2006. <a href="http://www.justice.gov/criminal/cybercrime/press-releases/2006/yePlea.htm">http://www.justice.gov/criminal/cybercrime/press-releases/2006/yePlea.htm</a> (accessed 05 16, 2013).

*USA TODAY*. "Three charged in Ericsson spy investigation in Sweden." *USA TODAY*. 05 08, 2003. <a href="http://usatoday30.usatoday.com/tech/news/2003-05-08-ericsson\_x.htm">http://usatoday30.usatoday.com/tech/news/2003-05-08-ericsson\_x.htm</a> (accessed 05 16, 2013).

Vijayan, Jaikumar. "Stuxnet renews power grid security concerns: First known SCADA malware program to target control systems prompts new questions about security of U.S. power grid." *NetworkWorld*. 07 26, 2010. <a href="http://www.networkworld.com/news/2010/072610-stuxnet-renews-power-grid-security.html">http://www.networkworld.com/news/2010/072610-stuxnet-renews-power-grid-security.html</a> (accessed 05 16, 2013).

Wallack, Todd. "EMC sues ex-employees to guard trade secrets." *Boston Business Journal*. 10 09, 2006. <a href="http://www.bizjournals.com/boston/stories/2006/10/09/story4.html?page=all">http://www.bizjournals.com/boston/stories/2006/10/09/story4.html?page=all</a> (accessed 05 16, 2013).

Warren, Peter. "Hunt for Russia's web criminals: The Russian Business Network -- which some blame for 60% of all internet crime -- appears to have gone to ground. But, asks Peter Warren, has it really disappeared?" *Guardian*. 11 15, 2007. <a href="http://www.guardian.co.uk/technology/2007/nov/15/news.crime">http://www.guardian.co.uk/technology/2007/nov/15/news.crime</a> (accessed 05 16, 2013).

Warrick, Joby, and Carrie Johnson. "Chinese Spy 'Slept' In U.S. for 2 Decades: Espionage Network Said to Be Growing." *Washington Post*. 04 03, 2008. <a href="http://www.washingtonpost.com/wp-dyn/content/story/2008/04/02/ST2008040204050.html">http://www.washingtonpost.com/wp-dyn/content/story/2008/04/02/ST2008040204050.html</a> (accessed 05 16, 2013).

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

# **Recent Developments in US Intellectual Property Law**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University

I've been updating chapters in the upcoming edition of a textbook and hope readers will find some of the research interesting. This week I'm posting materials I added to the chapter on intellectual property law.

## **AIA**

Peter E. Heuser of Schwabe, Williamoson & Wyatt summarized the American Invents Act (AIA) of 2011[1] as follows: "The AIA is the most important legislative patent reform in over 50 years. The AIA will change how patents are granted, how patent litigation will proceed and what kinds of inventions are eligible for patents, among other things."[2] The author summarized the main features of the AIA in detailed discussions of the following areas:

- First-to-file Will Now Establish Priority of Invention
- Prior Commercial User Defense is Established
- New Post-grant Proceedings for Patent Validity Challenges
- The PTO Will No Longer Grant Patents on Tax Strategy
- Special Transitional Review for Certain Patents Related to Financial Products and Services
- Most PTO Fees Will Increase By 15 Percent
- Limited Prioritized Examination Will be Available
- New Rules will Affect Litigation by Nonpracticing Entities
- False Patent Marking Claims are Curbed
- Other Provisions Will Make it More Difficult to Attack Patent Validity.

Complete information about the legislation is available through the Library of Congress THOMAS database.[3]

The PROTECT IP Act (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act)[4] or PIPA, was introduced in the US Senate in May 2011 but failed to make it to the floor of the Senate.[5] After extensive public opposition, including a worldwide temporary blackout of thousands of Websites in protest of PIPA and the Stop Online Piracy Act (SOPA, below),[6] the bill was suspended in January 2012 pending further analysis.[7]

PIPA's main points include the following (quoting several sections from the THOMAS database):

- Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 or the PROTECT IP Act of 2011 (Sec. 3) Authorizes the Attorney General (AG) to commence: (1) an in personam action against a registrant of a nondomestic domain name (NDN) used by an Internet site dedicated to infringing activities (ISDIA) or an owner or operator of an ISDIA accessed through an NDN; or (2) if such individuals are unable to be found by the AG or have no address within a U.S. judicial district, an in rem action (against a domain name itself, in lieu of such individuals) against the NDN used by an ISDIA.
- Defines ISDIA as a site that: (1) has no significant use other than engaging in or facilitating copyright infringement, circumventing technology controlling access to copyrighted works, or selling or promoting counterfeit goods or services; or (2) is designed, operated, or marketed and used to engage in such activities.
- Defines NDN as a domain name for which the registry that issued the domain name and operates the relevant top level domain, and the registrar for the domain name, are located outside the United States.
- Allows the court, upon application by the AG after an NDN-related in personam
  or in rem action is commenced under this section, to issue a temporary restraining
  order or an injunction against the NDN, registrant, owner, or operator to cease and
  desist further ISDIA activity if the NDN is used within the United States to access
  an ISDIA directing business to U.S. residents and harming U.S. intellectual
  property right holders.
- Directs the AG to identify and provide advance notice to operators of nonauthoritative domain name system servers (NDNSSs), financial transaction providers (FTPs), Internet advertising services (IASs), and providers of information location tools (ILTs), including search engines, online directories, and other indexes with hypertext links or referrals to online locations, whose action may be required to prevent such NDN-related ISDIA activity.
- Sets forth the preventative measures required to be taken by NDNSSs, FTPs, IASs, and ILTs upon being served with a court order in a such an NDN-related action commenced by the AG.

- (Sec. 4) Authorizes the AG or an intellectual property right owner harmed by an ISDIA to commence: (1) an in personam action against a registrant of an ISDIA's domain name or an owner or operator of an ISDIA accessed through a domain name; or (2) if such individuals are unable to be found or have no address within a U.S. judicial district, an in rem action against a domain name used by an ISDIA.
- Allows the court, upon application by the relevant plaintiff after an in personam or in rem action concerning a domain name is commenced under this section, to issue a temporary restraining order or injunction against a domain name, registrant, owner, or operator to cease and desist further ISDIA activity if the domain name is: (1) registered or assigned by a domain name registrar or registry located or doing business in the United States, or (2) used within the United States to access an ISDIA directing business to U.S. residents and harming U.S. intellectual property right holders.
- Directs the relevant plaintiff to identify and provide advance notice to FTPs and IASs whose action may be required to prevent such ISDIA activity.
- Requires, upon being served with a court order after such an in personam or in rem action concerning a domain name is commenced by the AG or a private right owner under this section: (1) FTPs to take reasonable specified preventative measures, and (2) IASs to take technically feasible and reasonable measures.
- Sets forth provisions regarding the entities that may be required to take certain preventative measures in actions concerning both domain names and NDNs: (1) granting immunity to such entities for actions complying with a court order, (2) authorizing the relevant plaintiff to bring an action for injunction relief against a served entity that knowingly and willfully fails to comply with a court order, and (3) permitting such entities to intervene in commenced actions and request modifications, suspensions, or terminations of related court orders.
- (Sec. 5) Provides immunity from liability for: (1) FTPs or IASs that, in good faith, voluntarily take certain preventative actions against ISDIAs, and (2) domain name registries and registrars, FTPs, ILTs, or IASs that, in good faith, withhold services from infringing sites that endanger public health by distributing prescription medication that is counterfeit, adulterated, misbranded, or without a valid prescription....

## **SOPA**

The Stop Online Piracy Act, H.R.3261,[8] is summarized in the THOMAS database as follows:

- ... Authorizes the Attorney General (AG) to seek a court order against a U.S.-directed foreign Internet site committing or facilitating online piracy to require the owner, operator, or domain name registrant, or the site or domain name itself if such persons are unable to be found, to cease and desist further activities constituting specified intellectual property offenses under the federal criminal code including criminal copyright infringement, unauthorized fixation and trafficking of sound recordings or videos of live musical performances, the recording of exhibited motion pictures, or trafficking in counterfeit labels, goods, or services.
- Sets forth an additional two-step process that allows an intellectual property right holder harmed by a U.S.-directed site dedicated to infringement, or a site promoted or used for infringement under certain circumstances, to first provide a written notification identifying the site to related payment network providers and Internet advertising services requiring such entities to forward the notification and suspend their services to such an identified site unless the site's owner, operator, or domain name registrant, upon receiving the forwarded notification, provides a counter notification explaining that it is not dedicated to engaging in specified violations. Authorizes the right holder to then commence an action for limited injunctive relief against the owner, operator, or domain name registrant, or against the site or domain name itself if such persons are unable to be found, if: (1) such a counter notification is provided (and, if it is a foreign site, includes consent to U.S. jurisdiction to adjudicate whether the site is dedicated to such violations), or (2) a payment network provider or Internet advertising service fails to suspend its services in the absence of such a counter notification.
- Requires online service providers, Internet search engines, payment network providers, and Internet advertising services, upon receiving a copy of a court order relating to an AG action, to carry out certain preventative measures including withholding services from an infringing site or preventing users located in the United States from accessing the infringing site. Requires payment network providers and Internet advertising services, upon receiving a copy of such an order relating to a right holder's action, to carry out similar preventative measures.
- Provides immunity from liability for service providers, payment network
  providers, Internet advertising services, advertisers, Internet search engines,
  domain name registries, or domain name registrars that take actions required by
  this Act or otherwise voluntarily block access to or end financial affiliation with
  such sites.
- Permits such entities to stop or refuse services to certain sites that endanger public health by distributing prescription medication that is adulterated, misbranded, or without a valid prescription.
- Expands the offense of criminal copyright infringement to include public performances of: (1) copyrighted work by digital transmission, and (2) work

intended for commercial dissemination by making it available on a computer network. Expands the criminal offenses of trafficking in inherently dangerous goods or services to include: (1) counterfeit drugs; and (2) goods or services falsely identified as meeting military standards or intended for use in a national security, law enforcement, or critical infrastructure application.

- Increases the penalties for: (1) specified trade secret offenses intended to benefit a foreign government, instrumentality, or agent; and (2) various other intellectual property offenses as amended by this Act.
- Directs the U.S. Sentencing Commission to review, and if appropriate, amend related Federal Sentencing Guidelines.
- Requires the Secretary of State and Secretary of Commerce to appoint at least one
  intellectual property attache to be assigned to the U.S. embassy or diplomatic
  mission in a country in each geographic region covered by a Department of State
  regional bureau.

Critics of the legislation include the American Civil Liberties Association, some educators, some law professors, and the United States Student Association.[9] Arguments included the following:

- The bill would lead to removal of much non-infringing content from the Web, resulting in infringement of free speech
- Eliminating the focus articulated in PIPA about concentrating on sites dedicated to infringing activity would waste government resources on an enormous range of sites
- Internet service providers, search engine providers, payment network providers and advertising services would all have to obey the Attorney General's orders to block all access to sites with infringing content, thus blocking access to all the sites' non-infringing content as well
- Educational uses could be severely constrained if a single infringing document led to the shutdown of an entire site
- Sites with a single link to infringing content could be classified as "facilitating" infringement and thus be shut down
- The bill would violate standards of due process by allowing administrative shutdown without providing an opportunity for the owners of the accused sites a chance to defend themselves

- SOPA's potential barriers to access could severely affect the worldwide movement to pressure dictatorial regimes such as that of the People's Republic of China in their consistent suppression of free access to information
- Librarians, educators and students could be subject to administrative shutdown even for what could be justified as fair use of copyright materials.

The proposed bill was dropped at the same time as PIPA (above).

## PATENT TROLLS

Groups aggressively targeting users of little-known patents, often purchased from inventors who have never exercised their rights before, are known as *non-practicing entities* or *patent trolls*. Some of these companies devote their entire business to suing or threatening to sue on the basis of their acquired patents.[10]

In one notorious case, a company bought "...the Canadian patent known as "Automatic Information, Goods, and Services Dispensing System (Canada '216)" whose complete text is available at <

http://patents1.ic.gc.ca/details?patent\_number=1236216&language=EN\_CA > [and] specifically addresses 'a system for automatically dispensing information, goods and services to a customer on a self-service basis including a central data processing centre in which information on services offered by various institutions in a particular industry is stored. One or more self-service information and sales terminals are remotely linked to the central data processing centre and are programmed to gather information from prospective customers on goods and services desired, to transmit to customers information on the desired goods or services from the central data processing centre, to take orders for goods or services from customers and transmit them for processing to the central data processing centre, to accept payment, and to deliver goods or services in the form of documents to the customer when orders are completed. The central data processing centre is also remotely linked to terminals of the various institutions serviced by the system, so that each institution can be kept up-dated on completed sales of services offered by that institution.' [Note that Canadian spelling is used above.] Think about this patent. Does it not remind you unavoidably of what you did the last time you ordered a book or bought something online? Or performed any other commercial transaction on the Web?"

A study published by the Boston University School of Law[11] found that patent trolls "...cost U.S. software and hardware companies US\$29 billion in 2011...."[12]

In the House of Representatives, Peter DeFazio (D-OR) introduced HR.6245, Saving High-Tech Innovators from Egregious Legal Disputes Act of 2012Saving High-Tech Innovators from Egregious Legal Disputes Act of 2012 in August 2012.[13] It would "[Amend] federal patent law to allow a court, upon finding that a party does not have a reasonable likelihood of succeeding in an action disputing the validity or alleging

infringement of a computer hardware or software patent, to award the recovery of full litigation costs to the prevailing party, including reasonable attorney's fees...." At the time of writing (May 2013) the bill was still in the hands of the Subcommittee on Intellectual Property, Competition and the Internet of the House Committee on the Judiciary.

In May 2013, Senator Charles Schumer (D-NY) introduced S.866, the Patent Quality Improvement Act, an amendment to the AIA to extend its provisions for challenging patents on business methods.[14]

The Library of Congress THOMAS database describes the substance of the proposal as follows:

Amends the Leahy-Smith America Invents Act to remove the eight-year sunset provision with respect to the transitional post-grant review program available to review the validity of covered business method patents, thereby making the program permanent.

Expands the term "covered business method patent" to include a patent that claims a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of any enterprise, product, or service, except technological inventions. (Current law limits the program to financial products or services.) [15]

### **END NOTES**

- [1] (US House of Representatives 2011)
- [2] (Heuser 2013)
- [3] (Library of Congress 2011)
- [4] (Library of Congress 2012)
- [5] (US Senate 2011)
- [6] (Weisman 2012)
- [7] (Timm 2012)
- [8] (Library of Congress 2011)
- [9] (Electronic Frontier Foundation 2011)
- [10] (Hachman 2013)
- [11] (Bessen and Meurer 2012)
- [12] (Essers 2012)
- [13] (Library of Congress 2012)
- [14] (Gross 2013)

### WORKS CITED

Bessen, James E., and Michael J. Meurer. "The Direct Costs from NPE Disputes: Abstract." *Social Science Research Network.* 06 28, 2012.

http://papers.ssrn.com/sol3/papers.cfm?abstract\_id=2091210## (accessed 05 18, 2013).

Electronic Frontier Foundation. "Documents about SOPA." EFF.ORG. 12 12, 2011. <a href="https://www.eff.org/search/site/sopa">https://www.eff.org/search/site/sopa</a> (accessed 05 17, 2013).

Essers, Loek. "'Patent Trolls' Cost Tech Companies \$29 Billion Last Year, Study Says." *PCWorld*. 06 27, 2012.

http://www.pcworld.com/article/258395/patent\_trolls\_cost\_tech\_companies\_29\_billion\_1 ast\_year\_study\_says.html (accessed 05 18, 2013).

Gross, Grant. "Senator introduces legislation targeting patent trolls." *PCWorld*. 05 01, 2013. <a href="http://www.pcworld.com/article/2037005/senator-introduces-legislation-targeting-patent-trolls.html">http://www.pcworld.com/article/2037005/senator-introduces-legislation-targeting-patent-trolls.html</a> (accessed 05 18, 2013).

Hachman, Mark. "Inside The Mind of A Patent Troll: If It's Legal, It Must Be OK." readwrite.com. 05 13, 2013. <a href="http://readwrite.com/2013/05/03/inside-the-mind-of-a-patent-troll-if-its-legal-it-must-be-ok">http://readwrite.com/2013/05/03/inside-the-mind-of-a-patent-troll-if-its-legal-it-must-be-ok</a> (accessed 05 18, 2013).

Heuser, Peter E. "Recent Developments in IP Law of Interest to Business Attorneys." Schwabe, Williamson & Wyatt. 02 26, 2013.

http://www.schwabe.com/showarticle.aspx?Show=12770 (accessed 05 17, 2013).

Kabay, M. E. "PanIP has rights: PanIP has patents on e-commerce-related systems." *NetworkWorld*. 04 15, 2003.

http://www.networkworld.com/newsletters/sec/2003/0414sec1.html (accessed 05 18, 2013).

Library of Congress. "Bill Summary & Status, 112th Congress (2011 - 2012): H.R.3261." http://thomas.loc.gov/cgi-bin/bdquery/z?d112:HR03261:@@@D&summ2=m&. October 26, 2011. http://thomas.loc.gov/cgi-bin/thomas (accessed 04 03, 2012).

- —. "Bill Summary & Status, 112th Congress (2011 2012): S.23." Library of Congress | THOMAS. 09 16, 2011. <a href="http://thomas.loc.gov/cgi-bin/bdquery/D?d112:3:./temp/~bdNMSP:@@@L&summ2=m&|/home/LegislativeData.php?n=BSS;c=112">http://thomas.loc.gov/cgi-bin/bdquery/D?d112:3:./temp/~bdNMSP:@@@L&summ2=m&|/home/LegislativeData.php?n=BSS;c=112</a> (accessed 05 17, 2013).
- —. "Bill Summary & Status, 112th Congress (2011 2012): S.968." Library of Congress | THOMAS. 01 23, 2012. <a href="http://thomas.loc.gov/cgi-bin/bdquery/z?d112:SN00968:@@@L&summ2=m&">http://thomas.loc.gov/cgi-bin/bdquery/z?d112:SN00968:@@@L&summ2=m&</a> (accessed 05 17, 2013).
- —. "Bill Summary & Status, 112th Congress (2011-2012): H.R.6245." Library of Congress | THOMAS. 08 14, 2012. <a href="http://thomas.loc.gov/cgi-bin/bdquery/D?d112:1:./temp/~bdIwEJ:@@@L&summ2=m&|/home/LegislativeData.php?n=BSS;c=112|">http://thomas.loc.gov/cgi-bin/bdquery/D?d112:1:./temp/~bdIwEJ:@@@L&summ2=m&|/home/LegislativeData.php?n=BSS;c=112|</a> (accessed 05 18, 2013).
- —. "Bill Summary & Status, 113th Congress (2013-2014): S.866." Library of Congress | THOMAS. 05 06, 2013. <a href="http://thomas.loc.gov/cgi-">http://thomas.loc.gov/cgi-</a>

bin/bdquery/D?d113:19:./temp/~bdpN5y:@@@L&summ2=m&|/home/LegislativeData.php?n=BSS;c=113| (accessed 05 18, 2013).

Timm, Trevor. "After Historic Protest, Members of Congress Abandon PIPA and SOPA in Droves." Electronic Frontier Foundation Deeplinks Blog. 01 19, 2012. <a href="https://www.eff.org/deeplinks/2012/01/after-historic-protest-members-congress-abandon-pipa-and-sopa-droves">https://www.eff.org/deeplinks/2012/01/after-historic-protest-members-congress-abandon-pipa-and-sopa-droves</a> (accessed 05 17, 2013).

US House of Representatives. "H.R. 1249 (112th): Leahy-Smith America Invents Act." govtrack.us. 09 16, 2011. <a href="http://www.govtrack.us/congress/bills/112/hr1249">http://www.govtrack.us/congress/bills/112/hr1249</a> (accessed 05 17, 2013).

US Senate. "S. 968 (112th): Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011." govtrack.us. 05 26, 2011. http://www.govtrack.us/congress/bills/112/s968/text (accessed 05 17, 2013).

Weisman, Jonathan. "After an Online Firestorm, Congress Shelves Antipiracy Bills." *New York Times*. 01 20, 2012. <a href="http://www.nytimes.com/2012/01/21/technology/senate-postpones-piracy-vote.html?r=0">http://www.nytimes.com/2012/01/21/technology/senate-postpones-piracy-vote.html?r=0</a> (accessed 05 17, 2013).

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.</a>
<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

# UPDATES ON SPAM, PHISHING AND TROJANS

M. E. Kabay, PhD, CISSP-ISSMP

In updating a chapter on spam, phishing and Trojans in a security textbook, I collected and inserted additional material that I am making available to readers here.

For 2012, Symantec reported that Android-operating-system threats (virtually unknown a decade earlier) against mobile devices increased drastically between January 2010 and the end of 2012: from fewer than 100 unique variants in about 10 families to around 4500 variants in about 170 families.[1] In addition, an increasing number of phishing scams in 2012 were being carried out through social media – a term not even mentioned in the corresponding report for the first half of 2006.[2]

\* \* \*

A notorious spammer was Sanford "Spamford" Wallace, founder of Cyber Promotions in the 1990s, which actively used spam as a commercial service. In October 2009, Facebook won a civil suit against him for sending fraudulent messages to its users.[3] Wallace was ordered to pay \$711M fine – which he was unlikely to pay because he filed for bankruptcy in June 2009.

In August 2011, he was indicted in the federal court in San Jose on

...multiple counts of fraud and related activity in connection with electronic mail. Wallace was also charged with three counts of intentional damage to a protected computer and two counts of criminal contempt. According to the indictment, from approximately November 2008 through March 2009, Wallace executed a scheme to send spam messages to Facebook users. Those messages compromised approximately 500,000 legitimate Facebook accounts, and resulted in more than 27 million spam messages being sent through Facebook's servers. The indictment alleges that Wallace sent spam messages to Facebook users during three time periods: First, on or about Nov. 5, 2008, and continuing until approximately Nov. 6, 2008, Wallace accessed Facebook's computer network to initiate the transmission of a program that resulted in more than 125,000 spam messages being sent to Facebook users; Second, on Dec. 28, 2008, Wallace accessed Facebook's computer network to initiate the transmission of a program that resulted in nearly 300,000 spam messages being sent to Facebook users; Third, on Feb. 17, 2009, Wallace accessed Facebook's computer network to initiate the transmission of a program that resulted in more than 125,000 spam messages being sent to Facebook users.[4]

At the time of writing (May 2013), USA v. Sanford Wallace was scheduled to open on Monday June 3, 2013 in the court of Judge Edward J. Davila in the San Jose Courthouse.[5]

Symantec reported about spam as over 90% of total email traffic in 2009[6] and 2010[7], but the proportion began dropping over the next few years. In June, 2011, Symantec reported a spam rate of about 73% of total email;[8] by December 2011, they reported a further drop to about 70%.[9] According to Kaspersky Lab in early 2013, "...the share of spam in email traffic decreased steadily throughout 2012 to hit a five-year low. The average for the year stood at 72.1% - 8.2 percentage points less than in 2011. Such a prolonged and substantial decrease in spam levels is unprecedented."[10] A different study in January 2013 suggested that only about 60% of all email was spam in 2012.[11] Estimates by other experts suggested that only about 15% of the total spam was getting through all the spam filters at ISP and application levels.[12]

In "The Economics of Spam" published in the Summer 2012 issue of the *Journal of Economic Perspectives*, Justin M. Rao (Microsoft) and David H. Reiley (Google), both formerly employees of Yahoo! Research, discuss the *externality* of spam – the use of victims' resources to support profit for the criminals. They write,

We estimate that American firms and consumers experience costs of almost \$20 billion annually due to spam. Our figure is more conservative than the \$50 billion figure often cited by other authors, and we also note that the figure would be much higher if it were not for private investment in anti-spam technology by firms.... On the private-benefit side, based on the work of crafty computer scientists who have infiltrated and monitored spammers' activity ... we estimate that spammers and spam-advertised merchants collect gross worldwide revenues on the order of \$200 million per year. Thus, the "externality ratio" of external costs to internal benefits for spam is around 100:1.[13]

\* \* \*

The Anti-Phishing Working Group (AWPG) was founded in 2003 and is one of the most active and productive anti-phishing organizations today:

The APWG is a worldwide coalition unifying the global response to cybercrime across industry, government and law-enforcement sectors. APWG's membership of more than 2000 institutions worldwide is as global as its outlook, with its directors, managers and research fellows advising: national governments; global governance bodies like ICANN; hemispheric and global trade groups; and multilateral treaty organizations such as the European Commission, Council of Europe's Convention on Cybercrime, United Nations Office of Drugs and Crime, Organization for Security and Cooperation in Europe and the Organization of American States. Membership is open to financial institutions, retailers, solutions providers, ISPs, telcos, defense contractors, law enforcement agencies, trade groups, treaty organizations and government agencies. APWG member benefits include: clearinghouses of cybercrime event data; cybercrime response utilities for professionals from the private, public, and NGO sectors who combat cybercrime; community-building conferences for cybercrime management professionals; public education utilities for cybercrime prevention; standards

development for cybercrime data exchange and programs for promotion of cybercrime research.[14]

\* \* \*

It was inevitable that spammers would adapt to filtering measures. By late 2012, an increasing number of spammers were distributing their spam among a large number of compromised servers, leading to the term *snowshoe spamming*. McAfee Labs summarized the problem as follows:

Snowshoe spamming is now one of the biggest spam problems. The issue has exploded over the past two years and will continue to increase sharply due to lack of exposure by law enforcement authorities and threats of lawsuits by companies using the illegal email lists.

The phenomenon is characterized by the following:

- Spammers blast out millions and millions of blatantly illegal spam messages every day from newly rented hosts until they get evicted from their subnetworks or move on.
- Recipients have their inboxes bombarded with these spam messages and are unable to opt out of them because they are not sent from a legitimate source.
- The result of snowshoe spamming is permanently blacklisted addresses and sometimes subnetworks.
- Because spamming is seen as simply annoying rather than malicious, authorities have largely ignored this problem, despite the growing volumes of unwanted email originating from these sources. Companies using these shady marketers have threated to file defamation lawsuits when researchers have tried to expose this activity.[15]

Criminals continue the evolution of their tools without respite; a January 2013 report found that spear phishers have applied a new tool called Bouncer that adapts their URLs to include unique identifiers for their intended victims; attempting to access the criminals' pages without a valid identifier in the URL results in a 404 (no such page) error, thus interfering with researchers' analysis of the phishing pages.[16]

In February 2013, analysts found that "When security experts looked into some of the highest profile hacks in recent years - one particular criminal group kept on coming to their attention. The Comment Group, which industry insiders say is based in China, offer hacking for hire – be it for individuals, corporations or governments...." They research individual companies or organizations to locate detailed information that allows highly specific topics and even content in the phishing messages. For example, a Coca-Cola executive reportedly opened a phishing email supposedly from his own boss; the link he clicked on downloaded spyware into his computer and allowed Chinese industrial spies to extract information which stymied the acquisition of China's largest soft-drinks company.[17]

In April 2013, the US Department of Homeland Security (DHS) warned "organizations that post a lot of business and personal information on public web pages and social media sites" not to do so. In October of 2012, phishers harvested detailed information about employees from a public posting by an energy company listing attendees at a conference. In addition to spear-phishing attacks on named individuals, "Malicious emails that appeared to be from one of the attendees were sent to others on the list informing them of a change in the sender's email address. Recipients were politely asked to click on an attached link that promptly took them to a site containing malware." [18]

The Anti Phishing Working Group (AWPG) is a valuable repository of statistical information about phishing.[19] Their report on phishing during the fourth quarter of 2013 includes the following findings (these are direct quotations formatted as bullet points with page references removed):

- Phishing attacks against online game players saw a massive increase, from 2.7 percent of all phishing attacks in Q3 to 14.7 percent in Q4.
- Financial services continued to be the most targeted industry sector in the fourth quarter of 2012 with payment services close behind.
- Online gaming credentials are valuable to certain criminals, who sell them on the black market. In-game items held in those accounts can also be sold by phishers for real-world cash. Victims can even have their real-life identities stolen.
- Attacks against social media doubled to 6%, up from 3% in the third quarter.
- During Q4, about 30 percent of personal computers worldwide were infected with malware.
- More than 57 percent of PCs in China may have been infected, while PCs in European nations were infected least often.
- Except for October 2012, the number of phishing sites declined every month from April 2012 through December 2012.
- April 2012 saw 63,253 unique phishing sites detected, falling to 45,628 in December 2012.
- The APWG received reports of 28,195 unique phishing sites in December. December's total was 31 percent lower than the high of 40,621 reports in August 2009.
- Use of crimeware dipped slightly in this quarter from the previous, as did the use of data-stealing malware.
- The use of other malware has increased by a statistically significant amount from the previous quarter.[20]

More recent reports about Trojans include the following cases and studies:

• The BackDoor.Wirenet.1 Trojan was identified in August 2012; the malware "is the first Trojan Horse program that works on the Mac OS X and Linux platforms

- that is 'designed to steal passwords stored by a number of popular Internet applications." [21]
- The "PandaLabs Q1 Report" for 2013 found that "Trojans set a new record, causing nearly 80 percent of all computer infections worldwide. Despite their inability to replicate, Trojans are capable of triggering massive infections through compromised Web sites that exploit vulnerabilities in browser plug-ins like Java, Adobe Reader, etc. This attack method allows hackers to infect thousands of computers in just a few minutes with the same Trojan or different ones, as attackers have the ability to change the Trojan they use based on multiple parameters such as the victim's location, the operating system used, etc."[22]
- In March 2013, Kaspersky Labs reported that a new spyware attack on Tibetan freedom activists used a Trojan designed for the Android mobile-phone operating system.[23]
- The Flashback Trojan had infected more than 600,000 Macintosh computers by early April 2013 by exploiting a flaw in Java.[24]
- In April 2013, criminals sent out invitations to watch video footage of the Boston Marathon bombings. A remote-access Trojan was installed as a "WinPcap Packet Driver (NPF)" to evade notice. [25]
- In May 2013, Graham Cluley of Sophos reported on a Trojan (Mal/BredoZp-B) circulated in an email supposedly from Tiffany & Co. that claimed to include details of an export license and a payment invoice.[26]

Finally, there's some interesting information on the underground economy in the following table from the Symantec "Fraud Activity Trends" published in 2010:

Table of Prices Paid for Data Traded in the Underground Economy[27]

Overall Rank		Item	Percentage		2010 Price Ranges
2010	2009		2010	2009	
1	1	Credit card information	22%	19%	\$0.07-\$100
2	2	Bank account credentials	16%	19%	\$10-\$900
3	3	Email accounts	10%	7%	\$1-\$18
4	13	Attack tools	7%	2%	\$5-\$650
5	4	Email addresses	5%	7%	\$1/MB-\$20/MB
6	7	Credit card dumps	5%	5%	\$0.50-\$120
7	6	Full identities	5%	5%	\$0.50-\$20
8	14	Scam hosting	4%	2%	\$10-\$150
9	5	Shell scripts	4%	6%	\$2-\$7
10	9	Cash-out services	3%	4%	\$200-\$500 or 50%-70% of total v

## NOTES

- [1] (Symantec 2013)
- [2] (Turner 2006)
- [3] (Associated Press 2009)
- [4] (FBI 2011)
- [5] (San Jose Federal Court 2013)
- [6] (McMillan 2009)
- [7] (Toor 2010)
- [8] (Henderson 2011)
- [9] (Whitney 2011)
- [10] (Kaspersky Lab 2013)
- [11] (Gudkova 2013)
- [12] (Radicati and Hoang 2012)

- [13] (Rao and Reiley 2012)
- [14] (Anti-Phishing Working Group 2013)
- [15] (McAfee 2012)
- [16] (VERACODE 2013)
- [17] (Lee 2013)
- [18] (Vijayan 2013)
- [19] (Anti-Phishing Working Group 2013)
- [20] (Aaron 2013)
- [21] (Kosner 2012)
- [22] (PandaLabs 2013)
- [23] (Gallagher 2013)
- [24] (Silverman 2012)
- [25] (Cluley, Sick malware authors exploit Boston Marathon bombing with Trojan attack 2013)
- [26] (Cluley 2013)
- [27] (Symantec 2010)

#### WORKS CITED

- Aaron, Greg. "Phishing Activity Trends Report: 4th Quarter 2012." *Anti-Phishing Working Group.* 04 24, 2013. http://docs.apwg.org/reports/apwg\_trends\_report\_Q4\_2012.pdf (accessed 05 23, 2013).
- Anti-Phishing Working Group. "About APWG." *APWG*. 2013. http://apwg.org/about-APWG/ (accessed 05 23, 2013).
- —. "APWG Phishing Attack Trends Reports." APWG. 04 24, 2013. http://apwg.org/resources/apwg-reports/ (accessed 05 23, 2013).
- Associated Press. "Sanford Wallace: Facebook Wins \$711 Million In Case Against 'Spam King'." *Huff Post | Tech.* 10 30, 2009. http://www.huffingtonpost.com/2009/10/30/sanford-wallace-facebook-\_n\_339703.html (accessed 05 23, 2013).
- Cluley, Graham. "Breakfast malware at Tiffany's? Trojan horses spammed out widely." *Sophos | nakedsecurity.* 05 22, 2013. http://nakedsecurity.sophos.com/2013/05/22/tiffany-malware/ (accessed 05 23, 2013).
- —. "Sick malware authors exploit Boston Marathon bombing with Trojan attack." *Sophos | nakedsecurity.* 04 17, 2013.

- http://nakedsecurity.sophos.com/2013/04/17/malware-boston-marathon-bombing/ (accessed 05 23, 2013).
- FBI. "Sanford Wallace Indicted for Spamming Facebook Users: Self-proclaimed "Spam King" Sent More Than 27 Million Spam Messages." FBI | San Francisco Division | US Attorney's Office | Northern District of California. 08 04, 2011. http://www.fbi.gov/sanfrancisco/press-releases/2011/sanford-wallace-indicted-for-spamming-facebook-users (accessed 05 23, 2013).
- Gallagher, Sean. "First targeted attack to use Android malware discovered: Kaspersky uncovers trojan spread by "spear-phish" to Tibet activists." *ars technica*. 03 26, 2013. http://arstechnica.com/security/2013/03/first-targeted-attack-to-use-android-malware-discovered/ (accessed 05 21, 2013).
- Gudkova, Darya. "Spam in January 2013." *Securelist | Analysis.* 02 21, 2013. http://www.securelist.com/en/analysis/204792282/Spam\_in\_January\_2013 (accessed 05 22, 2013).
- Henderson, Nicole. "Symantec Report Finds Spam Accounts for 73 Percent of June Email." *Web Host Industry Review.* 06 28, 2011. http://www.thewhir.com/web-hosting-news/symantec-report-finds-spam-accounts-for-73-percent-of-june-email (accessed 05 23, 2013).
- Kaspersky Lab. "Spam in 2012: Continued Decline Sees Spam Levels Hit 5-year Low." *Kaspersky Lab.* 01 13, 2013. http://www.kaspersky.com/about/news/spam/2013/Spam\_in\_2012\_Continued\_Decline\_Sees\_Spam\_Levels\_Hit\_5\_year\_Low (accessed 05 23, 2013).
- Kosner, Anthony Wing. "New Trojan Backdoor Malware Targets Mac OS X And Linux, Steals Passwords And Keystrokes." *Forbes | Tech.* 08 31, 2012. http://www.forbes.com/sites/anthonykosner/2012/08/31/new-trojan-backdoor-malware-targets-mac-os-x-and-linux-steals-passwords-and-keystrokes/ (accessed 05 23, 2013).
- Lee, Dave. "The Comment Group: The hackers hunting for clues about you." *BBC | News | Business*. 02 11, 2013. http://www.bbc.co.uk/news/business-21371608 (accessed 05 23, 2013).
- McAfee. "Snowshoe Spamming Emerges as Threat to Email Security." *McAfee | Business Home | Security Awareness.* 12 27, 2012. http://www.mcafee.com/us/security-awareness/articles/snowshoe-spamming-biggest-problem.aspx (accessed 05 23, 2013).
- McMillan, Robert. "90 percent of e-mail is spam, Symantec says." *Computerworld | Applications*. 05 26, 2009. http://www.computerworld.com/s/article/9133526/90\_percent\_of\_e\_mail\_is\_spam\_Symantec\_says (accessed 05 23, 2013).
- PandaLabs. "PandaLabs Q1 Report: Trojans Account for 80% of Malware Infections, Set New Record." *Panda Security | Press Room | News.* 05 03, 2013.

- http://press.pandasecurity.com/news/pandalabs-q1-report-trojans-account-for-80-of-malware-infections-set-new-record/ (accessed 05 23, 2013).
- Radicati, Sara, and Quoc Hoang. "Email Statistics Report, 2012-2016: Executive Summary." *Radicati Group.* 04 23, 2012. http://www.radicati.com/wp/wp-content/uploads/2012/08/Email-Statistics-Report-2012-2016-Executive-Summary.pdf (accessed 05 22, 2013).
- Rao, Justin M., and David H. Reiley. "The Economics of Spam." *Journal of Economic Perspectives 26(3):87-100.* 2012. http://www.aeaweb.org/articles.php?hs=1&fnd=s&doi=10.1257/jep.26.3.87 (accessed 05 23, 2013).
- San Jose Federal Court. "Calendar for Judge Edward J. Devila." *US Courts.* 05 23, 2013. http://www.cand.uscourts.gov/CEO/cfd.aspx?7143 (accessed 05 23, 2013).
- Silverman, Dwight. "More than half a million Macs infected with Flashback Trojan malware." *Chron | TechBlog.* 04 05, 2012. http://blog.chron.com/techblog/2012/04/more-than-half-a-million-macs-infected-with-flashback-trojan-malware/ (accessed 05 23, 2013).
- Symantec. "2013 Internet Security Threat Report, Volume 18." *Symantec | Security Response Publications.* 04 15, 2013. http://www.symantec.com/content/en/us/enterprise/other\_resources/b-istr\_main\_report\_v18\_2012\_21291018.en-us.pdf (accessed 05 22, 2013).
- —. "Fraud Activity Trends." Symantec | Enterprise | Security Response | Internet Security Threat Report. 2010. http://www.symantec.com/threatreport/topic.jsp?id=fraud\_activity\_trends&aid=u nderground\_economy\_servers (accessed 05 23, 2013).
- Toor, Amar. "Symantec Says 92-Percent of All E-mail is Spam, Phishing Attacks Declining." *SWITCHES*. 08 13, 2010. http://www.switched.com/2010/08/13/symantec-says-92-percent-of-all-e-mail-is-spam-phishing-attacks/ (accessed 05 22, 2013).
- Turner, Dean. "Symantec Internet Security Threat Report, Volume X." *Symantec | White Papers.* 09 22, 2006. http://eval.symantec.com/mktginfo/enterprise/white\_papers/ent-whitepaper\_symantec\_internet\_security\_threat\_report\_x\_09\_2006.en-us.pdf (accessed 05 22, 2013).
- VERACODE. "New Phishing Toolkit Uses Whitelisting To Keep Scams Alive." *VERACODE | the security ledger.* 01 16, 2013. https://securityledger.com/new-phishing-toolkit-uses-whitelisting-to-keep-scams-alive/ (accessed 05 23, 2013).
- Vijayan, Jaikumar. "DHS warns of spear-phishing campaign against energy companies: Attackers used information from company website to craft attacks." 

  Computerworld | Security | Malware and Vulnerabilities. 04 05, 2013. 

  http://www.computerworld.com/s/article/9238190/DHS\_warns\_of\_spear\_phishing\_campaign\_against\_energy\_companies (accessed 05 23, 2013).

Whitney, Lance. "Spam sinks to lowest level in almost three years, says Symantec: The amount of spam around the globe now accounts for 70 percent of all e-mail, a sharp decline from 2009 when it accounted for 90 percent." *c/net / news / security & Privacy*. 12 07, 2011. http://news.cnet.com/8301-1009\_3-57338317-83/spam-sinks-to-lowest-level-in-almost-three-years-says-symantec/ (accessed 05 23, 2013).

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

## Securing Shared Cloud-Based File Repositories M. E. Kabay, PhD, CISSP-ISSMP

Here's another block of material I added to a chapter as I'm editing a security textbook.

File-sharing services such as Dropbox and Google Drive have put effort into securing the data stored and shared by individuals and groups. For example, Dropbox answers the question "How secure is Dropbox?" as follows:

We have a dedicated security team using the best tools and engineering practices available to build and maintain Dropbox, and you can rest assured that we've implemented multiple levels of security to protect and back up your files. You can also take advantage of two-step verification, a login authentication feature which you can enable to add another layer of security to your account.

Other Dropbox users can't see your files in Dropbox unless you deliberately share links to files or share folders. Dropbox employees are prohibited from viewing the content of files you store in your account. Employees may access file metadata (e.g., file names and locations) when they have a legitimate reason, like providing technical support. Like most online services, we have a small number of employees who must be able to access user data for the reasons stated in our privacy policy (e.g., when legally required to do so). But that's the rare exception, not the rule. We have strict policy and technical access controls that prohibit employee access except in these rare circumstances. In addition, we employ a number of physical, technical, and heuristic security measures to protect user information from unauthorized access.[1]

Nonetheless, there are serious security concerns about cloud-based file-sharing tools and Dropbox in particular. At a Black Hat EU conference in 2013, the paper "DropSmack: How cloud synchronization services render your corporate firewall worthless" caught the eye of writer Michael Kassner. The paper summary included the following points:

- ....[C]loud-based synchronization solutions in general, and Dropbox in particular, can be used as a vector for delivering malware to an internal network."
- ...Dropbox synchronization service can be used as a Command and Control (C2) channel.
- ...[F]unctioning malware is able to use Dropbox to smuggle out data from exploited remote computers.

The paper's author, experienced penetration-tester Jacob Williams, warned that if a bad actor has any access to a secured Dropbox folder, it is possible to synchronize a remote-access Trojan he wrote called DropSmack with all the shared Dropbox folders. The tool would allow the infiltration of the entire corporate network. Williams also warned that access to a Dropbox folder by employees using their personal computers raises legal issues:

"Many general counsels are more than a little worried about the appearance of authorizing us to pen test what could end up being be home machines. That's becoming a sticky issue with pen-testers these days as people open spear phishing emails delivered to the corporate email addresses on machines that may be privately owned. "Many general counsels are more than a little worried about the appearance of authorizing us to pen test what could end up being be home machines. That's becoming a sticky issue with pen-testers these days as people open spear phishing emails delivered to the corporate email addresses on machines that may be privately owned."[2]

Integrated collaboration tools have another danger, especially for inexperienced users who don't take daily backups: deleting one or more files (or all of them) in a shared Dropbox folder will propagate the deletion to all users of the shared folder. If any one of the users keeps a daily backup, the entire group of users can be protected against disaster; if none of them do, they may be in serious difficulty. In a related issue, any user who moves the files out of the Dropbox folder into a local folder will wipe the data from all the other users' Dropbox folders too.[3]

In a 2012 article, Matthew J. Schwartz urged corporate uses to pay attention to Dropbox use among their employees. His five recommendations (with more details in the original article) are

- Monitor Dropbox use
- Compare cloud service security
- Beware lackluster security cloud practices
- Treat Dropbox as a public repository
- Beware insider data exfiltration.[4]

A free tool, Cloudfogger, automatically encrypts data on the client side when it is uploaded to any external collaboration tool using 256 bit AES encryption. The tool then automatically decrypts the data when it is downloaded by an authorized user.[5]

#### NOTES

- [1] (Dropbox 2013)
- [2] (Kassner 2013)
- [3] (Kabay 2013)
- [4] (Schwartz 2012)
- [5] (Cloudfogger 2012)

#### **WORKS CITED**

- Cloudfogger. "Protect Your Privacy on SkyDrive, Dropbox, Google Drive in the Cloud." cloudfogger. 2012. http://www.cloudfogger.com/en/ (accessed 05 25, 2013).
- Dropbox. "How secure is Dropbox?" Dropbox. 2013. https://www.dropbox.com/help/27/en (accessed 05 25, 2013).
- Kabay, M. E. "Dropping the Ball on Dropbox." InfoSec Perception. 04 19, 2013. http://resources.infosecskills.com/perception/dropping-the-ball-on-dropbox/ (accessed 05 25, 2013).
- Kassner, Michael. "DropSmack: Using Dropbox to steal files and deliver malware." TechRepublic | Security. 04 15, 2013. http://www.techrepublic.com/blog/security/dropsmack-using-dropbox-to-steal-files-and-deliver-malware/9332 (accessed 05 25, 2013).
- Schwartz, Matthew J. "5 Dropbox Security Warnings For Businesses." InformationWeek | Security. 08 14, 2012. http://www.informationweek.com/security/management/5-dropbox-security-warnings-for-business/240005413?pgno=1 (accessed 05 25, 2013).

\* \* \*

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

# **Inadvertent Covert Channels**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University

The editing marathon continues. A chapter on instant messaging and collaboration tools prompted the following thoughts.

One morning a few weeks ago, I looked at my Skype icon and found that there had been a Skype call the night before. I found two 10-minute messages left on "voice-mail" through Skype several hours after I shut down my computer. The first couple of minutes was a perfectly normal recorded message from a colleague – but the remaining 18 minutes were sounds from his office! He had forgotten to terminate the call, so Skype obediently recorded everything the microphone could hear. I don't know if he noticed at all, because the second call was exactly 10:00 minutes long – an unlikely length had he terminated the session deliberately. I still have no idea what happened to prevent a third segment from being recorded.

This incident was unusual only in that it was a voice-mail recording. There are many times I have been in a Skype conversation, either with or without video, and have had to terminate the call myself because the person who initiated it forgot to click the red "end call" symbol. Failing to do so creates an unintentional covert channel for data transfer – which usually doesn't matter in casual conversations but which could be a serious problem in a business context.

A covert channel is a data transfer medium that is not known to the data owner. For example, a wiretap on a phone line or a man-in-the-middle attack on a wireless data connection are covert channels. Steganography, in which some tools insert the desired message into the low-order bits for pixel colours, is an example of using a covert channel for data transfer.

Another danger with instant-messaging clients is that the focus of one's typing can shift from a password-entry field into an instant-messaging field without one's notice; I have personally felt like (OK, been) a complete fool for typing password into a Skype message – and sending it (thankfully) to my wife, who very kindly purged the Skype history for our conversations. Imagine if I had done that to the Skype message field for anyone else! I can see it now: someone posts a screenshot of my password in their Skype client – if I thought that libelling a computer manufacturer by mistake a few years ago was bad, such an error would surely have increased the number of hits for "Kabay idiot" in Google to astronomical levels.

A common covert channel when people use faxes (and apparently, there were 16B faxes sent last year!)< <a href="http://www.slideshare.net/RingCentral/facts-about-global-fax-usage">http://www.slideshare.net/RingCentral/facts-about-global-fax-usage</a> > is to send the fax to the wrong fax number. In 2006, a report surfaced that "A small Lockport, Manitoba-based distributor of herbal remedies has for the past 15 months been mistakenly receiving faxes containing confidential information belonging to hundreds of patients with Prudential Financial Inc.'s insurance group. The data exposed in the breach -- and faxed to the company by doctors and clinics across the U.S. -- included the patients' Social Security numbers, bank details and health care information."<

http://www.computerworld.com/s/article/108429/Confidential\_patient\_data\_sent\_to\_wrong\_company\_for\_15\_months?taxonomyId=017 > The doctors and clinics were using the wrong number

for their faxes – only one digit different from that of the insurance company – and swamping the tiny North Regents company with thousands of unwanted, highly confidential faxes. Prudential insisted that its fax number was correctly indicated on all its documents and correspondence, and said that it could not be held responsible for misdialling by its customers. Indeed, the large company told the small company that "Effective immediately, North Regent RX will forward to Prudential Financial all faxes it has received, as well as any it may receive in the future." This solution was wholly impractical for the tiny group, who offered to change their toll-free number if Prudential would pay for the costs of reprinting all its advertising, business cards and letterhead. Prudential declined to do so.

Some people (I am, with effort, refraining from characterizing their degree of intelligence) use old email messages as a basis for sending out new ones using the REPLY ALL function – and without verifying whether the distribution list is appropriate. Simply choosing the wrong list can also lead to trouble, as Sherri Goforth discovered when that Tennessee Republican bigot (no hesitation here) sent a racist image sneering at President Obama to "the wrong list" – and had it posted on the Web.< <a href="http://www.cnn.com/2009/POLITICS/06/16/tennessee.email/">http://www.cnn.com/2009/POLITICS/06/16/tennessee.email/</a>>

Another inadvertent covert channel is simply hitting REPLY ALL by mistake – and sending inappropriate messages to people who shouldn't receive them. In 2010, an advertising director wrote a message using inappropriate ("locker-room" was his term) language to criticize colleagues to a teammate in an internal competition – and used REPLY ALL by mistake, sending the email to 200 people – including the people he was criticizing.<
a href="http://online.wsj.com/article/SB10001424052748703386704576186520353326558.html">http://online.wsj.com/article/SB10001424052748703386704576186520353326558.html</a> And then there's the problem of a REPLY ALL message asking "Take me off this list" or "You used REPLY ALL, you fool" and generating waves of angry third- and fourth-level REPLY ALLs. In January 2009, someone in the US State Department sent a blank message with several thousand recipients visible in the TO or CC field; replies using REPLY ALL caused a denial of service by swamping the internal email servers.<
a href="http://www.huffingtonpost.com/2009/01/10/replyall-email-storm-hits\_n\_156856.html">http://www.huffingtonpost.com/2009/01/10/replyall-email-storm-hits\_n\_156856.html</a> >

Basic good sense to avoid inadvertent covert channels in email include using the BCC field for the distribution list to prevent foolish distribution of replies.

For more guidance in effective use of email, see "Using E-mail Safely and Well" <a href="http://www.mekabay.com/infosecmgmt/emailsec.pdf">http://www.mekabay.com/infosecmgmt/emailsec.pdf</a> >

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:mekabay@gmail.com">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2013 M. E. Kabay. All rights reserved.

## **Cloud Computing and Production Systems**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University

In the continuing series of additions to chapters in a security textbook, here's one of the sections I wrote about production controls and cloud computing.

The history of production computing is repeating itself: in the 1960s through the 1980s, computers were so physically large and hugely expensive that many smaller organizations contracted with *service bureaus* to access computing resources. Connections in physically close locations (e.g., city cores) were often through physical coaxial cable or twisted pair connections. For more distant connections, clients linked their *dumb terminals* to the *mainframes* through telephone lines using *modems*. Sometimes the switched telephone connections through the *plain old telephone service* (POTS) were fixed in place and dedicated to the connection – hence they were called *dedicated lines*.

Today, as we approach the middle of the 2010s, the speed of Internet connections is reaching 10 Gbps – an enormous bandwidth that facilitates remote access to banks of computing power of almost unimaginable power.[1] Organizations are capitalizing on the possibility of creating virtual machines (virtualization) that insulate concurrent processes from each other, allowing far more efficient sharing of centralized resources than running processes on dedicated systems inhouse. Inexpensive computers (thin clients) with relatively little application software and local disk storage can be used to access all the necessary programs and data required for the organization's business through access to cloud services.

In March 2013, industry analysts said, "More than 60% of all enterprises will have adopted some form of cloud computing in 2013, according to Gartner Research. The cloud market is slated to grow to \$131 billion worldwide this year, or 18.5% over the \$111 billion last year. In its 2013 State of the Cloud Report that surveyed over 1200 IT professionals, IT-reseller CDW found 39% of organizations are already using some form of cloud solution, an 11% increase over 2011."[2]

IDC reported that "In coming years, the economic impact of cloud computing will be vast. Each year a greater percentage of businesses IT budgets are earmarked for cloud. An expansive study by the International Data Corporation (IDC)... reported that, in 2011, businesses spent \$28 billion on public cloud IT services. Amazingly, the spending on public cloud expected to surpass \$207 billion worldwide by 2016...." The researchers analysed trends in specific industries:

- Banking: increasing use of cloud computing
- Healthcare: slower adoption
- Manufacturing: particularly strong growth for customer relationship management (CRM) and among smaller businesses
- Insurance: increasing use

• Communications/media: particularly strong user of storage-on-demand.[3]

Gartner also predicted that, "... by 2015, 10% of overall IT security enterprise capabilities will be delivered in the cloud, with the focus today clearly on messaging, Web security and remote vulnerability assessment. However, there's also the expectation there will be more on the way, such as data-loss prevention, encryption, authentication available too as technologies aimed to support cloud computing mature." [4]

As with service bureaus of yesteryear, cloud computing poses special challenges for operations security and production controls.

- The reliability of employees hired to handle confidential and critically important data is out of the hands of the client organization.
- Management policies, monitoring, software maintenance, audits all are potentially handled exclusively by employees of the cloud-computing provider.
- Bring-your-own-device (BYOD) practices are facilitated by access to remote cloud services.
- Quality of service (QoS) issues and details of the service-level agreements (SLAs) complicate the contractual relations between providers and customers.

Cloud computing, like service bureaus, can provide cost-effective growth paths for smaller business and can offload information technology used for IT functions that are not viewed as mission-critical, allowing IT staff to concentrate on innovative, highly productive applications that can differentiate an organization in its marketplace. They allow for graded increases in computing power without forcing organizations to follow step-functions with large investments in much bigger equipment and increased operational costs. However, extending one's IT infrastructure into centres run by separate entities with their own profit motives requires careful attention to security. At a minimum, organizations should implement the following recommendations for maintaining adequate controls over their production environment when it is in a remote site using cloud computing:

- 1. During evaluations of multiple vendors, be sure to contact clients of each firm to have personal discussions of their experience with the providers' service level agreements and performance, openness of communications about production controls, cooperation in site visits, and adequacy and cooperation in resolving problems.
- 2. Examine the adequacy of encryption for all stored proprietary data. No cleartext data should be accessible to employees of the cloud-hosting company at any time including while decrypted on the virtual machines running on their servers.
- 3. Be sure that virtual private networks are in place for all Internet-based data transfers.
- 4. Explicitly discuss update standards for all the software your organization plans to run on the cloud service. Are you responsible for such updates or is the cloud vendor?
- 5. Be sure that all software running in the cloud on behalf of the customer organization

- respects the terms of the vendors' licenses. For example, be sure that a one-user license is not being applied to a thousand concurrent virtual machines on your behalf.
- 6. Understand and analyse the business-continuity planning (BCP) and disaster-recovery planning (DRP) in place to ensure continued operations on your behalf should there be problems at the cloud vendor's site(s). Are the exact terms spelled out to your satisfaction in the contracts? Are there provisions for testing the adequacy of the BCP and DRP?
- 7. Ensure that the contract allows for external audits which can be initiated by the client. Independent evaluation of the security, QoS and continuity of operations (CoO) is essential for the protection of the client.
- 8. Discuss the vendors' security policies and practices, including real-time monitoring for breaches (situational awareness), handling malware, and vulnerability analysis, including penetration testing.
- 9. Evaluate the billing processes carefully: what determines the periodic invoicing concurrent users? Total number of sessions? Detailed algorithms measuring such elements as disk I/O, CPU cycles, swapping to and from virtual memory, or bandwidth utilization? Model the costs if possible using detailed information from your own existing systems.

#### **NOTES**

- [1] Bandoim, L. "Growth of Cloud Computing and ERP Continues to Accelerate." *Technorati | Technology | Cloud Computing* (2013-05-04). http://technorati.com/technology/cloud-computing/article/growth-of-cloud-computing-and-erp/
- [2] Nain, A. "With The Cloud Market Set To Flirt With 20% Growth In 2013, How Can You Play It?" *Seeking Alpha*, 2013-03-20. <a href="http://seekingalpha.com/article/1291461-with-the-cloud-market-set-to-flirt-with-20-growth-in-2013-how-can-you-play-it">http://seekingalpha.com/article/1291461-with-the-cloud-market-set-to-flirt-with-20-growth-in-2013-how-can-you-play-it</a>
- [3] Weeks, J. "Vertical Markets 2013 Growth Predictions for Cloud Computing." *US Signal Blog*, 2013-01-16. <a href="http://blog.ussignalcom.com/blog-1/bid/259630/Vertical-Markets-2013-Growth-Predictions-for-Cloud-Computing">http://blog.ussignalcom.com/blog-1/bid/259630/Vertical-Markets-2013-Growth-Predictions-for-Cloud-Computing</a>
- [4] Messmer, E. "Gartner: Growth in cloud computing to shape 2013 security trends: Gartner predicts by 2015, 10% of overall IT security enterprise capabilities will be delivered in the cloud." *Network World*, 2012-12-06. <a href="http://www.networkworld.com/news/2012/120612-gartner-cloud-security-264873.html">http://www.networkworld.com/news/2012/120612-gartner-cloud-security-264873.html</a>

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2013 M. E. Kabay. All rights reserved.

## **Notes on Improving Website Security**

## by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems

## **School of Business & Management**

## **Norwich University**

The editing marathon continues. Here are a couple of additions I made to a chapter on Website security.

#### **Embedded Identifiers in URLs**

Sometimes registration or unsubscribe messages include personalized URLs; for example, "To unsubscribe, click on < http://www.some-company.com/unusbscribe/?=12345 >. The problem is that the identifying code (12345 in the example) can be replaced by any other number – and some of the generated numbers will unsubscribe other subscribers. Another unfortunate use of such a technique occurs in email messages for participation in Webinars; sometimes the coded URL in the email goes directly to a registration page with information filled in – information such as the precise name, email address, and employer information drawn from the database of previous contacts.

In general, it is poor practice to provide such short identifiers that a user or a simple program or batch file could be used to delete valid records in a database or to harvest confidential data from a Website. For example, a simple html file in Adobe Acrobat can be used to force the program to access every URL in the file; if a malefactor has created, say, 20,000 unique identifiers and all or most of them are affiliated with real people, the malefactor could easily affect the accounts or collect the information shown on the customer-specific pages.

To avoid such problems, either create an address space with far more possible identifier values than a 1:1 mapping of real accounts to identifiers; e.g., for a 100,000-person list, use generated values using a string of 20 positions with 94 values per position available in uppercase, lowercase, numbers, and special characters, resulting in 94^20 = 10^39 keyspace, far beyond anything manageable by an amateur.

### **Browser-Platform Security**

An increasingly important platform for considerations of Website security is smart phones. By the end of 2012,

There were 2.1 billion mobile Web users in the world at the end of 2012.

According to estimates by The ITU (June, 2012), there were 2.1 billion active mobile-broadband subscriptions in the world. That is 29.5 percent of the global population.

Mobile-broadband subscriptions have grown 40 percent annually over the last three years.

Mobile-broadband subscription outnumber fixed broadband subscriptions 3:1.

In developed countries mobile-broadband users often also have access to a fixedbroadband connection, but in developing countries mobile broadband is often the only access method available to people.

Ericsson (November 2012) forecasts that global mobile broadband subscriptions will reach 1.5 billion at the end of 2012, and 6.5 billion in 2018. The mobile phone will continue to be the dominant mobile broadband access device. [1]

Tablets also have their own versions of browsers. Web designers are increasingly having to cope with significant differences among platforms accessing their code.

Craig Smith included the following points in a January 2013 article entitled, "Optimizing Ecommerce for Tablets and Smartphones:"

- Improving navigation and usability: users should be able to select options easily and correctly; avoid drop-down menus and buttons that are close together.
- Leveraging responsive design: determine how to present the Website according to what kind of device is accessing it.
- Determining the purpose of the access: distinguish between the types of queries that are most common and different across platforms. Optimize design for the most common types for each platform.[2]

Another question is whether ecommerce sites should depend on Web access or develop applications (apps) specifically for smartphone and tablet operating systems. A major advantage of apps is that they can be programmed to avoid the vulnerabilities common to mobile devices in these early years of widespread adoption.

#### **Notes:**

[1] C. Smith, "Optimizing Ecommerce for Tablets and Smartphones." Practical ecommerce (2013-01-15). <a href="http://www.practicalecommerce.com/articles/3869-Optimizing-Ecommerce-for-Tablets-and-Smartphones">http://www.practicalecommerce.com/articles/3869-Optimizing-Ecommerce-for-Tablets-and-Smartphones</a>

[2] D. Traxler, "Mobile Commerce: Website or App?" Practical ecommerce (2013-01-01). http://www.practicalecommerce.com/articles/3862-Mobile-Commerce-Website-or-App-

#### For Further Reading:

Anderson, R. Security Engineering: A Guide to Building Dependable Distributed Systems, 2<sup>nd</sup> edition. Wiley, 2008.

Bhargav, A. and B. V. Kumar. Secure Java: For Web Application Development. CRC Press, 2010.

Cobb, Stephen. Privacy for Business: Web Sites and Email. Dreva Hill, 2002.

Elliott, E. *Programming JavaScript Applications: Robust Web Architecture With Node, HTML5, and Modern JS Libraries.* O'Reilly Media, 2013.

Gabarro, S. A. Web Application Design and Implementation: Apache 2, PHP5, MySQL, JavaScript, and Linux/UNIX, 2<sup>nd</sup> edition. Wiley, 2013.

Gookin, D. Android Phones for Dummies. For Dummies, 2013.

Gunasekera, S. Android Apps Security. Apress, 2012.

Harwani, B. M. Android Programming Unleashed. Sams, 2012.

Kissoon, T. Securing Web Applications. Auerbach, 2013.

- Long, F., D. Mohindra, R. C. Seacord, D. F. Sutherland and D. Svoboda. *The CERT Oracle Secure Coding Standard for Java*. Addison-Wesley Professional, 2011.
- Mark, D., A. Horovitz, K. Kim and J. LaMarche. *More iOS 6 Development: Further Explorations of the iOS SDK*. Apress, 2012.
- McGraw, G., and E. Felten. *Securing Java: Getting Down to Business with Mobile Code* 2<sup>nd</sup> edition. Wiley, 1999.
- Musciano, C., B. Kennedy and E. Weyl. *HTML5: The Definitive Guide*, 7<sup>th</sup> edition. O'Reilly Media, 2014.
- Scambray, J., Shema, M., and C. Sima. *Hacking Exposed Web Applications*, 2nd ed. San Francisco, CA: McGraw-Hill Osborne Media, 2006.
- Six, J. Application Security for the Android Platform: Processes, Permissions, and Other Safeguards. O'Reilly Media, 2011.
- Sullivan, B. Web Application Security, A Beginner's Guide. McGraw-Hill Osborne Media, 2011.
- Welling, L. and L. Thomson. *PHP and MySQL Web Development*, 5th Edition. Addison-Wesley Professional, 2013.
- Zalewski, M. *The Tangled Web: A Guide to Securing Modern Web Applications*. No Starch Press, 2011.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2013 M. E. Kabay. All rights reserved.

# **Stored-Data Security**

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University

Yet another chapter bites the dust: this week I have some additions to a chapter on stored-data security.

\* \* \*

## Addition and footnote to a section on "Volume Encryption and Encrypting File Systems:"

I/O to and from the mounted volume can be significantly slower than from an unencrypted disk drive. For example, observations in June 2013 showed that mounting an entire 7 GB partition encrypted by Symantec PGP Desktop v10.20.0 took ~7 seconds. In comparison, the same 7 GB of data encrypted using WinZip and 256-bit AES encryption took about an hour to decrypt in toto on a 7200 rpm two-disk performance RAID 0 set running under 64-bit Windows 7 Professional SP 1 on a 3.2 GHz AMD Phenom<sup>TM</sup> II X4 955 quad-core processor with 12 GB of RAM. Copying a 1.23 GB file took 85 seconds (~15 MB/sec) on the PGP encrypted volume (located on the RAID 0 hard drive) but only 20 seconds (~63 MB/sec) on the RAID 0 itself.

\* \* \*

## **New section on "Smart-Phone Encryption:"**

Users may store confidential information on mobile phones and tablets; typical entries include contact entries with phone numbers and sometimes with ancillary sensitive data such as passwords, personally identifiable information (e.g., government-issued identification numbers), and call records. Such devices may also be used as if they were flash drives, with potentially gigabytes of sensitive data downloaded from other sources and carried in a pocket, briefcase or handbag – and therefore easy to steal or to lose.

Another factor that can be significant for some users is that under US law at the time of writing in June 2013, a suspect who is questioned, interrogated or arrested cannot normally be forced to divulge the decryption code.[1]

Phones using Android 2.3.4 or later usually come with integrated total encryption; the process typically takes about an hour, ideally starts with a fully charged battery and connection to a power supply, and must not be interrupted. Interruption of this encryption process can damage or delete the data stored on the phone and requires a factory reset that wipes all current data and personal settings from the device.[2]

Apple iOS and Microsoft Windows Phone 7 also include encryption functions with varying coverage. Third-party software is available for all the operating systems discussed above.[3]

In March 2013, researchers at the Friedrich-Alexander University discovered how to access data encrypted on a version of the Android operating system:

The team froze phones for an hour as a way to get around the encryption system that protects the data on a phone by scrambling it.... The attack allowed the researchers to get at contact lists, browsing histories and photos.... [They] put Android phones in a freezer for an hour until the device had cooled to below -10C. ... [Q]uickly connecting and disconnecting the battery of a frozen phone forced the handset into a vulnerable mode. This loophole let them start it up with some custom-built software rather than its onboard Android operating system. The researchers dubbed their custom code Frost - Forensic Recovery of Scrambled Telephones.[15]

#### **REFERENCES:**

- [1] Radia, R., "Why you should always encrypt your smartphone." ArsTechnica (2011-01-16). http://arstechnica.com/gadgets/2011/01/why-you-should-always-encrypt-your-smartphone/
- [2] How-To Geek, "How to Encrypt Your Android Phone and Why You Might Want To." (2013). http://www.howtogeek.com/141953/how-to-encrypt-your-android-phone-and-why-you-might-want-to/
- [3] UNC-Chapel Hill, "Encrypting Cell Phones." University of North Carolina at Chapel Hill | Help & Support (2013-03-19). http://help.unc.edu/help/encrypting-cell-phones/
- [4] BBC, "Frozen Android phones give up data secrets: Freezing an Android phone can help reveal its confidential contents, German security researchers have found." BBC News | Technology (2013-03-07). http://www.bbc.co.uk/news/technology-21697704

\* \* \*

#### Some additions to the list of suggested readings:

Griffin, D. The Four Pillars of Endpoint Security: Safeguarding Your Network in the Age of Cloud Computing and the Bring-Your-Own-Device Trend. CreateSpace Independent Publishing Platform, 2013.

EMC Education Services. *Information Storage and Management: Storing, Managing, and Protecting Digital Information in Classic, Virtualized, and Cloud Environments* 2<sup>nd</sup> edition. Wiley, 2012.

Hitachi Data Systems. *Storage Concepts: Storing And Managing Digital Data*, Volume 1. HDS Academy, 2012.

Loshin, P. Simple Steps to Data Encryption: A Practical Guide to Secure Computing. Syngress, 2013.

Souppaya, M. and K. Scarfone. *Guidelines for Managing the Security of Mobile Devices in the Enterprise*. NIST Special Publication SP800-124 Revision 1. 2013-06. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2013 M. E. Kabay. All rights reserved.

# CLOUD STORAGE: RISKS AND REWARDS (1)

## By Jérémy Legendre

Jérémy Legendre is a brilliant student in computer security at Norwich University's School of Business and Management. He submitted an excellent paper on cloud storage for his IS340 Introduction to Information Assurance class in Fall 2012 and has graciously allowed us to publish his work here. Everything that follows is M. Legendre's with minor edits by Mich. The work is split into two parts for publication in this series.

#### Introduction

Backing up to the cloud means putting your backups on a remote server that can be accessed by Internet connection.[1] You can access your information from anywhere you have an Internet connection without taking up space on your machine's hard drive. Many businesses have started to use cloud computing and it is expected that there will be a "26 percent growth in adoption over the next several years".[2] However, the cloud is not *just* for businesses; even the U.S. government has started to adopt the cloud model. Cloud storage is offered for personal use (for free or fee) by a number of companies including Apple (iCloud), Dropbox and Google (Google Drive). With massive adoption of cloud backups users are increasingly concerned about how secure this backup method is.[3] With 100 percent adoption of cloud backups, everything will be available from anywhere. How much should you trust the cloud?

## Why has Cloud Storage Become Popular?

Cloud storage is not a new way to backup your files. The idea was first introduced in the 1960s by computer scientists John McCarthy and J.C.R. Licklider.[4] So why has cloud storage only become popular in recent years?

Prior to the 1990s, bandwidth and what we consider decent transfer rates were rare. In the 1970s, typical transfer speeds (for those who had the Internet) were around 300 bits per second, [5] – 27 seconds per kilobyte or approximately eight hours per megabyte. These speeds are not adequate for transferring large amounts of data. Furthermore, few people had access to the Internet during the 1970s and even into the early 1990s. For example, only two percent of households in the U.S. had access in 1994 and only twenty-six percent had access in 1998.[6] There was not much of a market for personal cloud storage services.

Online storage services started to spring up as bandwidth and speeds increased and more people started using the Internet.[7] Among the first to popularize this service was Dropbox, Inc. in 2007.[8] They pioneered seamless operating system integration, competitive prices and even offered a free plan with limited options. Dropbox created the industry standard for remote backup services.[9] Apple's iCloud storage service launched in 2011 and Google Drive in 2012.

Dropbox alone had four million users in February 2010[10] and more than one hundred million users as of November 2012.[11] Apple's iCloud hit over 190 million users in October of 2012[12] and Google Drive announced their ten million-user mark in June 2012.[13]

#### **Risks**

Cloud storage may be convenient but is your data secure? No matter which cloud storage service you choose, the services "have full access to your data and control where it is stored".[14] Cloud servers have been compromised, causing uncertainty or data compromise for customers.

## **Dropbox Compromises**

Although Dropbox is currently the face of personal cloud storage, it is not because they are the most secure. Back in July 2011 Dropbox announced that a code update had "completely disabled the authentication system for an unknown period of time".[15] That means that for a few hours, anyone could access any Dropbox account without any credentials. For many of us, that is a pretty scary thought. Although Dropbox reassured us that they are "implementing additional safeguards to prevent this from happening again", they were compromised once again in July 2012.[16]

The July 2012 compromise ended with a small number of customers' accounts being subject to unauthorized access. Sound familiar? Dropbox launched a full investigation and announced "that usernames and passwords recently stolen from other websites were used to sign in to a small number of Dropbox accounts. This may not sound like it is their fault but one of the accounts accessed was "an employee Dropbox account containing a project document with user email addresses". The email addresses acquired were then spammed. Since the 2012 compromise Dropbox has added an optional two-factor authentication system that sends a temporary code to your phone needed to log in and a "new page that lets you examine all active logins to your account". [17] Dropbox has not, to date reported any compromises since the attack.

#### iCloud Compromise

The iCloud compromise was a scary glimpse into the reality of what a little social engineering and loosely followed internal policies can lead to. In one hour Mat Honan's "entire digital life was destroyed".[18] Hackers social engineered their way into Honan's iCloud account by calling AppleCare and using his email address, billing address and last four digits of his credit card as identification.[19]

The hackers obtained his billing address from a simple and public *whois* lookup. From there they called Amazon (who also has a cloud storage service) and asked to change the email address on the account to an email address the hackers had access to. Amazon did so without a problem after the hacker provided Honan's billing address as identification. The hackers were able to reset the password on the Amazon account by having password reset information sent to the newly changed email and get hold of the last four digits of his credit card once inside.[20]

They now had enough information to fulfil AppleCare's identification requirements and get into Honan's iCloud account. Once the hackers were in Honan's iCloud account they were able to "reset his iCloud password, reset his Gmail password, gain control of his Twitter account".[21] Sadly, this is not the end of the destruction of Honan's "digital life". Honan had Find my iPhone turned on for his iPhone/iPad and Find my Mac[22] turned on for his MacBook Air. This is a service that allows you to locate your lost or stolen Apple products and even remotely wipe those devises, which is exactly what the attackers did.

Although this attack was not a technological one, this says a lot about how careful Apple really is with your account. Strict enforcement of policies to prevent social engineering attacks like this one is a must in any company holding sensitive information. Do not let this one isolated incident taint your decision-making. There have not been any other breaches reported since this incident and none before.

## **Google Drive Compromises**

There have been no major Google Drive compromises to date. A user reported on Google's support forum that he received a legitimate email from Google saying there was an "unauthorized attempt to login" to his account from Shanghai. Another user reported the same problem in the thread.[23] Luckily, the hackers were not able to access either of these accounts but what would happen if they were to get in?

Google states in their Terms of service that "Anything that has been permanently deleted from Google Drive by the owner, or if the owner's account was deleted, can't be recovered. It's also not possible to recover anything in Google Drive after a Google Apps domain administrator deletes someone's account." [24] In the event your Google Drive is compromised and wiped, there is *nothing* you can do to get your files back.

Google Drive seems like the safest choice on the surface but you risk losing everything you have ever backed up onto your account if there is a breach.

#### **END NOTES**

- [1] (Freedman 2012)
- [2] (Clancy)
- [3] (Krossman)
- [4] (Mohamed)
- [5] (12ht)
- [6] (National Science Foundation)
- [7] (Rhea, Wells and Eaton)
- [8] (Dropbox, Inc)
- [9] (Zelman)
- [10] (Ying)
- [11] (Constine)
- [12] (Lardinois)

[13] (Crook) [14] (Schwartzberg) [15] (Bott) [16] (Ferdowsi) [17] (Kerr) [18] (Honan) [19] (Kerr, Apple Responds to Journalist's iCloud Attack) [20] (Manjoo) [21] (Rose) [22] (Apple, Inc.) [23] (Google Support Forum) [24] (Google, Inc) \* \* \*

More next week.

\* \* \*

### Works Cited in Parts 1 & 2

Apple, Inc. "Find my iPhone, iPad, and Mac." (2012-11-13) http://www.apple.com/icloud/features/find-my-iphone.html

Bott, Ed. "Why I Switched from Dropbox to Windows Live Mesh." ZDnet (2011-04-07) http://www.zdnet.com/blog/bott/why-i-switched-from-Dropbox-to-windows-livemesh/3512

Box Cryptor. 16 November 2012 https://www.boxcryptor.com/

Clancy, Heather. "Cloud storage and backup: Is it safe?" (2012-02-20). http://www.zdnet.com/debate/cloud-storage-and-backup-is-it-safe/10086847/

Constine, Josh. "Dropbox Is Now The Data Fabric Tying Together Devices For 100M Registered Users Who Save 1B Files A Day." TechCrunch (2012-11-13). http://techcrunch.com/2012/11/13/Dropbox-100-million/

Crook, Jordan. "Google Drive Now Has 10 Million Users: Available On iOS and Chrome OS." TechCrunch (2012-06-28). http://techcrunch.com/2012/06/28/google-drive-now-has-10-million-users-available-on-ios-and-chrome-os-offline-editing-in-docs/

CSGNetwork. CSGNetwork. <a href="http://www.csgnetwork.com/bandwidth.html">http://www.csgnetwork.com/bandwidth.html</a>

Dropbox, Inc. "About Dropbox." Dropbox, Inc. https://www.Dropbox.com/about

Ferdowsi, Arash. "Yesterday's Authentication Bug.: (2011-06-20). <a href="https://blog.Dropbox.com/?p=821">https://blog.Dropbox.com/?p=821</a>

Freedman, A. Computer Desktop Encyclopedia. <a href="http://www.computerlanguage.com/">http://www.computerlanguage.com/</a>

General Services Administration. "GSA Launches Effort to Transition Federal Government to Cloud Computing." (2012-06-06). <a href="http://www.gsa.gov/portal/content/136575">http://www.gsa.gov/portal/content/136575</a>

Google Support Forum. "Google password hacked from China - anybody had similar issues after installing Google Drive?" (2012-09-19).

https://productforums.google.com/forum/?fromgroups=#!topic/drive/4- Hvz20mBY

Google, Inc. "File deletion and recovery policy."

http://support.google.com/drive/bin/answer.py?hl=en&answer=2405957

Honan, Mat. "How Apple and Amazon Security Flaws Led to My Epic Hacking." Wired (2012-08-06). <a href="http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/">http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/</a>

Jefferies, Charles P. "Google Drive vs. Dropbox: Ranking the Top 6 File Sync Services" *Backupify* (2012-05-17). <a href="http://blog.backupify.com/2012/05/17/ranking-the-top-online-file-sync-services/">http://blog.backupify.com/2012/05/17/ranking-the-top-online-file-sync-services/</a>

Kerr, Dara. "Apple Responds to Journalist's iCloud Attack." *C/net* (2012-06-08). <a href="http://news.cnet.com/8301-1009\_3-57487873-83/apple-responds-to-journalists-icloud-hack/">http://news.cnet.com/8301-1009\_3-57487873-83/apple-responds-to-journalists-icloud-hack/</a>

Kerr, D. "Dropbox Confirms it was Hacked, Offers Users Help." *C/net* (2012-7-31). <a href="http://news.cnet.com/8301-1009-3-57483998-83/Dropbox-confirms-it-was-hacked-offers-users-help/">http://news.cnet.com/8301-1009-3-57483998-83/Dropbox-confirms-it-was-hacked-offers-users-help/</a>

Krossman, Rachel. "Users report cloud storage security concerns in surveys." *TechTarget | SearchCloudStorage* (2011-11-21).

http://searchcloudstorage.techtarget.com/news/2240111421/Users-report-cloud-storage-security-concerns-in-surveys-more-news

Kumar, Mohit. "90% SSL sites vulnerable to the BEAST SSL attack." *The Hacker News* (2012-04-09). <a href="http://thehackernews.com/2012/04/90-ssl-sites-vulnerable-to-beast-ssl.html">http://thehackernews.com/2012/04/90-ssl-sites-vulnerable-to-beast-ssl.html</a>

Lardinois, Frederic. "Apple's iCloud Now Has Over 190M Users, Up From 150M Last Quarter And Seeing Steady Growth." *TechCrunch* (2012-10-25).

http://techcrunch.com/2012/10/25/apples-icloud-now-has-190-million-users/

Maltais, Michelle. "Future of Computing: The tablet and cloud will be king report says." *Los Angeles Times* (2012-04-23). <a href="http://articles.latimes.com/2012/apr/23/business/la-fi-tn-tablets-forrester-report-20120423">http://articles.latimes.com/2012/apr/23/business/la-fi-tn-tablets-forrester-report-20120423</a>

Manjoo, Farhad. "How not to get Hacked: The four things you need to do right now to avoid the fate of tech writer Mat Honan." (2012-07-08).

http://www.slate.com/articles/technology/technology/2012/08/mat honan the four things you need to do right now to avoid getting hacked .html

Mohamed, Arif. "A History of Cloud Computing: Cloud computing has evolved through a number of phases which include grid and utility computing, application service provision (ASP), and Software as a Service (SaaS)." *ComputerWeekly* (2012-11-13). <a href="http://www.computerweekly.com/feature/A-history-of-cloud-computing">http://www.computerweekly.com/feature/A-history-of-cloud-computing</a>

National Science Foundation. "The Sociodemographics of Access and Adoption." (2012-11-13). <a href="http://www.nsf.gov/statistics/nsf01313/socio.htm">http://www.nsf.gov/statistics/nsf01313/socio.htm</a>

Peterson, Peter A. H. and Peter Reiher. "CS448. Lab 3: Network Attacks." (2011. 15 11). <a href="http://mathcs.slu.edu/~chambers/spring11/security/assignments/lab04.html">http://mathcs.slu.edu/~chambers/spring11/security/assignments/lab04.html</a>

Process Software. "A Comparison of Secure File Transfer Mechanisms." (2008-04-03). <a href="http://www.process.com/tcpip/sft.pdf">http://www.process.com/tcpip/sft.pdf</a>

Rhea, Sean, et al. "Maintenance-Free Global Data Storage." *IEEE Internet Computing*, (Sep-Oct 2001). <a href="http://www.oceanstore.org/publications/papers/pdf/ieeeic.pdf">http://www.oceanstore.org/publications/papers/pdf/ieeeic.pdf</a>

Rose, Michael. "Hacked iCloud Password Leads to Nightmare." TUAW (2012-08-04). http://www.tuaw.com/2012/08/04/hacked-icloud-password-leads-to-nightmare/

Schwartzberg, David. "Cloud Storage Data Risks and Encryption." *nakedsecurity* (2012-08-03). <a href="http://nakedsecurity.sophos.com/2012/03/08/cloud-storage-data-risks-and-encryption/">http://nakedsecurity.sophos.com/2012/03/08/cloud-storage-data-risks-and-encryption/</a>

SSL. "What is SSL?" <a href="http://info.ssl.com/article.aspx?id=10241">http://info.ssl.com/article.aspx?id=10241</a>

Top 10 Cloud Storage. "The Importance of Data Encryption in Cloud Storage." (2012-11-16). <a href="http://www.top-10-cloud-storage.com/the-importance-of-data-encryption-in-cloud-storage/">http://www.top-10-cloud-storage.com/the-importance-of-data-encryption-in-cloud-storage/</a>

Ying, Jon. "Dropbox Around the World!" (2012-11-13). <a href="https://blog.Dropbox.com/?p=339">https://blog.Dropbox.com/?p=339</a>

Zelman, Josh. "How Dropbox got its First 10 million Users." *TechCrunch* (2011-11-01). <a href="http://techcrunch.com/2011/11/01/founder-storie-how-Dropbox-got-its-first-10-million-users/">http://techcrunch.com/2011/11/01/founder-storie-how-Dropbox-got-its-first-10-million-users/</a>

\* \* \*

#### **BIO**

Jeremy Legendre < mailto:jlegendre@stu.norwich.edu > is a currently entering his third year of studies in Norwich University's Bachelor of Science in Computer Security and Information Assurance (BSCSIA) program< http://programs.norwich.edu/business/csia/ > and hopes eventually to work with the US Department of Defense in cyber security. He has been programming since the age of thirteen and developed an antivirus for Mac OS X in the summer of 2012. He has always had a passion for technology and hopes to continue to an enjoyable and prosperous career in IT.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="http://www.mekabay.com/">http://www.mekabay.com/</a> >

# CLOUD STORAGE: RISKS AND REWARDS (2)

## By Jérémy Legendre

This is the second of two articles by Jérémy Legendre, a brilliant student in computer security at Norwich University's School of Business and Management. He submitted an excellent paper on cloud storage for his IS340 Introduction to Information Assurance class in Fall 2012 and has graciously allowed us to publish his work here. Everything that follows is M. Legendre's with minor edits by Mich.

## **Security of Data Transfers**

During transfer is the only time that your files are out of both your and your provider's hands. Your data can be captured and read or modified during transfer using a man-in-the-middle (MitM) attack if not encrypted.[1] Most cloud services have a secure socket layer for safer file transfer.[2] Do not choose a service without a valid SSL certificate.<sup>3</sup> You can encrypt files yourself before you upload them to your storage device but encrypted transfer is one step safer and practical. There are a few different ways to upload your data depending on your provider.

#### **FTP**

FTP or File Transfer Protocol had its first standard in 1971, prior to TCP/IP's existence. "FTP has traditionally used clear text passwords." [4] Your login information can be read by anyone running a MitM attack between you and your provider's server; even if your data is encrypted your credentials can still be compromised. [4] Alternatively, there is SFTP that uses a secure shell to encrypt your credentials when logging in.

#### **SSL**

"SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser." This means that if your cloud storage service's website has a valid SSL certificate, any information sent from your browser to the server and vice versa is encrypted. [5] There was a vulnerability in SSL that allowed hackers to strip the encryption that has been fixed but many service providers have yet to update their versions of SSL.[6] Be sure to check the encryption offered by a service before subscribing.

## **Encryption in Storage**

"As innovators like Apple and Microsoft, Google and Amazon, turn their customers on to the benefits of storing in the cloud, the importance of data encryption steps to the forefront."[7] You can back up any legal file you would like to your cloud storage including tax forms, utility bills, pay stubs, ebill receipts and medical records. These are files you do not want getting out as they may contain sensitive information like credit card numbers, social security numbers, addresses, phone numbers, email addresses which can all be used for identity theft.

Many cloud storage providers have built in storage encryption for no extra charge.<sup>26</sup> You can also encrypt your files yourself or use an additional cloud storage encryption service such as Box Cryptor for additional security.[8] SSL tunnels only encrypt your data during the transfer to your cloud storage server, so your data will be readable by anyone who compromises your account if there is no encryption during storage.

## Cloud Storage and the U.S. Government

The U.S. government has even started using the cloud. In June 2012, The U.S. General Services Administration launched an "Effort to Transition Federal Government to Cloud Computing"[9] Before this announcement the General Services Administration had already accomplished two things:

#### "1. First to Move Email to the Cloud:

Last year, GSA was the first federal agency to move to a cloud based email system, which has saved \$2 million dollars in costs so far. In addition, email system operating costs are expected to see additional 50 percent in savings with an estimated \$15 million in savings over five years.

2. Working to Standardize Security of Cloud Services:

FedRAMP is an initiative to standardize security assessments of cloud products and services. By addressing one of the key barriers to cloud adoption, this program will accelerate adoption by federal agencies. It will allow agencies to share authorizations, saving time and money otherwise spent on duplicative security reviews."<sup>33</sup>

## During the next year they are:

"3. Working on Blanket Purchase Agreements for the Federal Government:

Everything agencies need to move to the cloud is available right now through GSA. The products currently available from GSA include data storage, virtual machines, and web hosting. GSA is working to provide more cloud services to federal agencies, including email services."33

## **Concluding Remarks**

Cloud storage is the future of storing digital data and early adopters will benefit in the long run.[10] However, you must make sure your data is well protected. This chart, which M. E. Kabay and I have put together, may help you see which service might best fit your needs.

SERVICE	FUNCTIONS	OPTIONS	CAPACITY	COST	BACKUPS	SECURITY	PLATFORMS
ADrive	Files, sharing	Personal, Business, Adrive Enterprise	50 GB - 10 TB - unlimited	free- \$7/mo - \$16/mo	Manual	SSL transfer for paid services	PCs, Mac, Unix
BACKBLAZE	System, versions, locate stolen computer	Personal	unlimited	\$5/mo	Continuous, scheduled, or manual	encrypted on client; user- added key	Windows, Mac
BackupGenie	Automated backup, versions, sharing	Home, Business, Partners	75 GB, 250 GB, unlimited	\$5/mo, \$7/mo, \$10/mo	daily	SSL transfer, 256bit AES storage	Windows, Mac, iPad, iPhone
BackupandSha re	Automated backup, versions, sharing	Individual, Business	10 GB, unlimited	free, \$50/mo, \$150/mo	daily or manual	SSL transfer	Windows, Mac, iPad, iPhone, Android, Windows Mobile
backupify   Google Apps	backup, restore, search	Professional, Enterprise, Enterprise +	unlimited	\$3/user-mo, \$4/user-mo, \$990/domain -mo	daily or manual	SSL transfer, storage	Google Apps domains
backupify   Salesfore	backup, restore, search, export	Professional, Enterprise, Unlimited Salesforce	1 GB/user	\$50/mo for 10 users base + \$5/user-mo additional	daily or manual	SSL transfer, storage	Salesforce CRM software
backupify   Personal Apps	backup, restore	MyCloud Personal, 100 & 500	1 GB, 10 GB, 50 GB	free, \$5/mo, \$20/mo	weekly, nightly	SSL transfer, storage	Facebook, Twitter, Gmail, Google Drive, Google Calendar, Google Sites, Google Contacts, Flickr, Picasa, LinkedIn, Blogger, Zoho
Barracuda	backup appliance, cloud, private cloud, revisions history, restore	Models 190, 390, 490, 690, 890, 990, 1090	from 500GB to 80 TB	from \$1,000 to \$135,000	total control	SSL transfer, storage	Windows
Box							
Box Backup	open-source software	n/a	n/a do-it- yourself	free	total control	SSL transfer, storage	UNIX, Windows
Carbonite	backup, restore	Home, HomePlus, HomePremier, Business, BusinessPremier	unlimited, 250 GB, 500 GB	\$60/year through \$600/yr	continuous or scheduled	SSL, Blowfish storage; user- added key	Windows, Mac

SERVICE	FUNCTIONS	OPTIONS	CAPACITY	COST	BACKUPS	SECURITY	PLATFORMS
CRASHPLAN	backup, restore, versions, multiple storage sites	CRASHPLAN, CRASHPLAN+, CRASHPLANPR O, CRASHPLANPR Oe	unlimited	free through \$25/yr; also perpetual licenses — e.g., \$3,000 for 50 users + annual support	daily	encrypted on client; user- added key	Windows, Mac, Linux, Solaris
Dropbox	sharing, backups, restore, two factor authorization	Free, Pro, Teams	2 GB up to 1 TB	free through \$63,000 for 500 users	continuous	by client	Windows, Mac Linux, iPad, iPhone, Android and BlackBerry.
Druva	sharing, backups, restore, data analytics, remote deactivation	Professional, Enterprise, Unlimited	15 GB/user up to 100 GB/user	\$6/user-mo up	scheduled	SSL transfer, 256bit AES storage	Windows, Mac Linux, iPad, iPhone, Android and BlackBerry.
egnyte	local cloud, file server, file sharring, file transfer/FTP, remote file access, mobile apps, third party integration	Group, Office, Business, Enterprise	150 GB up to 3 TB	\$24.99/mont h - \$129.99/mon th. Enterprise: \$12.99/empl oyee/month	continuous or scheduled	SSL transfer, 256bit AES encryption in transit and at rest,	PC, Mac, iÓS, Android, Windows Mobile, WebOS
Elephantdrive	web access, secure sharing/sending,	Free, Personal, Business	2 GB up to 2 TB	Free - \$169.95/mon th, Variation in Business Tier	Automated	256bit AES encryption, optional personal key encryption	PC, Mac, Android (Beta), NAS
Google Drive	web access, OS integration	Free, 25 GB, 100 GB, Peronalized Plan	5 GB up to 16 TB	Free - \$799.99/mon th	N/A	SSL transfer	PC, Mac, Android, iOS
lBackup	API for 3rd party developers	n/a	10 GB up to 300 GB	\$9.95/month - \$299.95/mon th	N/A	SSL transfer, 256-bit AES encryption	PC, Mac, Linux, Android, iOS
iCloud	iTunes, Photo Stream, Documents, Safari, Calendar, Contacts, Mail, Apps, iBooks, Backup, Restor, Find my iPhone, Find my Friends	n/a	5 GB up to 55 GB	Free - \$100/year	Automatic	SSL Transfer, 128-bit AES encryption	Mac, iOS
Jungle Disk	web access	Personal, Business	Unlimited	\$2/month - \$5/month + \$0.15/GB	Automatic	AES-256 encryption	PC, Mac, iOS
Justcloud	sync multiple computers, web access, file sharing, mobile	n/a	Unlimited	n/a	Automatic	265 Bit Encryption	PC, Mac, iOS, Android, Blackberry

SERVICE	FUNCTIONS	OPTIONS	CAPACITY	COST	BACKUPS	SECURITY	PLATFORMS
Keepit	backup history, restore from backup, replicated backups,	Home Plan, Business Plan	Unlimited	£4.95/month - \$49.00/mont h	Automatic	256-bit Rijndael encryption	PC, Mac, Linux
livedrive	Reseller options	Backup, Briefcase, Pro Suite, Business	Unlimited, 2 TB, 10TB+	\$7.95/month - \$159.95/mon th	Automatic	"256-bit military grade encryption"	PC, Mac, Android, iOS
Microsoft SkyDrive	remote access, version tracking, online slide shows	n/a	7 GB up to 107 GB	Free - \$50.00/year	Automatic	SSL transfer	PC, Mac, Windows Phone, Android, iOS
mimedia	access media on demand, music, photo, and video streaming	Free, Premium	7 GB up to 100 GB	Free - \$4.99/month	Automatic	SSL transfer, NSA level 256-bit encryption	PC, Mac, iOS, Android
Mozy	local backup service, bandwidth throttling, web based and DVD restore, server support, custom domain, custom install	Home, Pro, Enterprise	50 GB - 1 TB	\$5.99/month/ computer - \$379.99/mon th/computer	Automatic	SSL transfer, 256-bit AES encryption	Mac, PC, iOS, Android
MyOtherDrive	collaboration, secure links, DDL for your files, USB drive backup	Free, Pro, Enterprise	2 GB - 10 TB	Free - \$2,400/year	Automatic	SSL transfer, AES 128-bit	PC, Mac
myPCBackup	multiple computer sync, web access, free trial, file versioning	n/a	unlimited	Pay-as-you- go	Automatic	SSL transfer	PC, Mac, iOS, Android, Blackberry
OpenDrive	file sync, web access	Personal, Business	5 GB - 1 TB (custom plan available)	Free - \$25/month	Manual	SSL transfer, custom encryption	PC, Mac, iOS, Android
PennyBackup	fast backups, free software, data recovery	n/a	unlimited	\$0.089/GB	Manual	256-bit AES encryption	PC
\$3	Encryption client, versioning	Free, Paid	5 GB - Unlimited	Free - Pay as you go	Manual	SSL transfer, server side encryption	n/a
SOS Online Backup	Mobile bakcup	Home, Business	5 GB - 2 TB	\$79.99/year - \$7,490.00/ye ar	Manual	military-grade encryption	PC, Mac, NAS, iOS, Android

SERVICE	FUNCTIONS	OPTIONS	CAPACITY	COST	BACKUPS	SECURITY	PLATFORMS
SugarSync	Sync multiple devices, mobile apps, remote access, outlook integration, versioning	n/a	5 GB - Custom	Free - Custom	Manual	SSL transfer, 128-bit AES server side encryption	PC, Mac, iOS, Android, Kindle, Symbian
Zip cloud	Sync multiple computers, web access	Personal, Business, Partner	75 GB - 5 TB	\$4.95/month - \$791.20/mon th	Automated	256bit SSL encryption	PC, Mac, iOS, Android, Blackberry

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

#### **NOTES**

- [1] (Peterson and Reiher)
- [2] (Kabay and Legendre)
- [3] (Jefferies)
- [4] (Process Software)
- [5] (SSL)
- [6] (Kumar)
- [7] (Top 10 Cloud Storage)
- [8] (Box Cryptor)
- [9] (General Services Administration)
- [10] (Maltais 2012)

#### Works Cited in Parts 1 & 2

Apple, Inc. "Find my iPhone, iPad, and Mac." (2012-11-13) <a href="http://www.apple.com/icloud/features/find-my-iphone.html">http://www.apple.com/icloud/features/find-my-iphone.html</a>

Bott, Ed. "Why I Switched from Dropbox to Windows Live Mesh." ZDnet (2011-04-07) <a href="http://www.zdnet.com/blog/bott/why-i-switched-from-Dropbox-to-windows-live-mesh/3512">http://www.zdnet.com/blog/bott/why-i-switched-from-Dropbox-to-windows-live-mesh/3512</a>

Box Cryptor. 16 November 2012 <a href="https://www.boxcryptor.com/">https://www.boxcryptor.com/</a>

Clancy, Heather. "Cloud storage and backup: Is it safe?" (2012-02-20). <a href="http://www.zdnet.com/debate/cloud-storage-and-backup-is-it-safe/10086847/">http://www.zdnet.com/debate/cloud-storage-and-backup-is-it-safe/10086847/</a>

Constine, Josh. "Dropbox Is Now The Data Fabric Tying Together Devices For 100M Registered Users Who Save 1B Files A Day." *TechCrunch* (2012-11-13). <a href="http://techcrunch.com/2012/11/13/Dropbox-100-million/">http://techcrunch.com/2012/11/13/Dropbox-100-million/</a>

Crook, Jordan. "Google Drive Now Has 10 Million Users: Available On iOS and Chrome OS." *TechCrunch* (2012-06-28). <a href="http://techcrunch.com/2012/06/28/google-drive-now-has-10-million-users-available-on-ios-and-chrome-os-offline-editing-in-docs/">http://techcrunch.com/2012/06/28/google-drive-now-has-10-million-users-available-on-ios-and-chrome-os-offline-editing-in-docs/</a>

CSGNetwork. CSGNetwork. <a href="http://www.csgnetwork.com/bandwidth.html">http://www.csgnetwork.com/bandwidth.html</a>

Dropbox, Inc. "About Dropbox." Dropbox, Inc. <a href="https://www.Dropbox.com/about">https://www.Dropbox.com/about</a>

Ferdowsi, Arash. "Yesterday's Authentication Bug.: (2011-06-20). <a href="https://blog.Dropbox.com/?p=821">https://blog.Dropbox.com/?p=821</a>

Freedman, A. Computer Desktop Encyclopedia. http://www.computerlanguage.com/

General Services Administration. "GSA Launches Effort to Transition Federal Government to Cloud Computing." (2012-06-06). <a href="http://www.gsa.gov/portal/content/136575">http://www.gsa.gov/portal/content/136575</a>

Google Support Forum. "Google password hacked from China - anybody had similar issues after installing Google Drive?" (2012-09-19).

https://productforums.google.com/forum/?fromgroups=#!topic/drive/4- Hvz20mBY

Google, Inc. "File deletion and recovery policy."

http://support.google.com/drive/bin/answer.py?hl=en&answer=2405957

Honan, Mat. "How Apple and Amazon Security Flaws Led to My Epic Hacking." Wired (2012-08-06). <a href="http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/">http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/</a>

Jefferies, Charles P. "Google Drive vs. Dropbox: Ranking the Top 6 File Sync Services" *Backupify* (2012-05-17). <a href="http://blog.backupify.com/2012/05/17/ranking-the-top-online-file-sync-services/">http://blog.backupify.com/2012/05/17/ranking-the-top-online-file-sync-services/</a>

Kerr, Dara. "Apple Responds to Journalist's iCloud Attack." *C/net* (2012-06-08). <a href="http://news.cnet.com/8301-1009-3-57487873-83/apple-responds-to-journalists-icloud-hack/">http://news.cnet.com/8301-1009-3-57487873-83/apple-responds-to-journalists-icloud-hack/</a>

Kerr, D. "Dropbox Confirms it was Hacked, Offers Users Help." *C/net* (2012-7-31). <a href="http://news.cnet.com/8301-1009-3-57483998-83/Dropbox-confirms-it-was-hacked-offers-users-help/">http://news.cnet.com/8301-1009-3-57483998-83/Dropbox-confirms-it-was-hacked-offers-users-help/</a>

Krossman, Rachel. "Users report cloud storage security concerns in surveys." *TechTarget | SearchCloudStorage* (2011-11-21).

http://searchcloudstorage.techtarget.com/news/2240111421/Users-report-cloud-storage-security-concerns-in-surveys-more-news

Kumar, Mohit. "90% SSL sites vulnerable to the BEAST SSL attack." *The Hacker News* (2012-04-09). <a href="http://thehackernews.com/2012/04/90-ssl-sites-vulnerable-to-beast-ssl.html">http://thehackernews.com/2012/04/90-ssl-sites-vulnerable-to-beast-ssl.html</a>

Lardinois, Frederic. "Apple's iCloud Now Has Over 190M Users, Up From 150M Last Quarter And Seeing Steady Growth." *TechCrunch* (2012-10-25).

http://techcrunch.com/2012/10/25/apples-icloud-now-has-190-million-users/

Maltais, Michelle. "Future of Computing: The tablet and cloud will be king report says." *Los Angeles Times* (2012-04-23). <a href="http://articles.latimes.com/2012/apr/23/business/la-fi-tn-tablets-forrester-report-20120423">http://articles.latimes.com/2012/apr/23/business/la-fi-tn-tablets-forrester-report-20120423</a>

Manjoo, Farhad. "How not to get Hacked: The four things you need to do right now to avoid the fate of tech writer Mat Honan." (2012-07-08).

http://www.slate.com/articles/technology/technology/2012/08/mat honan the four things you need to do right now to avoid getting hacked .html

Mohamed, Arif. "A History of Cloud Computing: Cloud computing has evolved through a number of phases which include grid and utility computing, application service provision (ASP), and Software as a Service (SaaS)." *ComputerWeekly* (2012-11-13). <a href="http://www.computerweekly.com/feature/A-history-of-cloud-computing">http://www.computerweekly.com/feature/A-history-of-cloud-computing</a>

National Science Foundation. "The Sociodemographics of Access and Adoption." (2012-11-13). <a href="http://www.nsf.gov/statistics/nsf01313/socio.htm">http://www.nsf.gov/statistics/nsf01313/socio.htm</a>

Peterson, Peter A. H. and Peter Reiher. "CS448. Lab 3: Network Attacks." (2011. 15 11). http://mathcs.slu.edu/~chambers/spring11/security/assignments/lab04.html

Process Software. "A Comparison of Secure File Transfer Mechanisms." (2008-04-03). <a href="http://www.process.com/tcpip/sft.pdf">http://www.process.com/tcpip/sft.pdf</a>

Rhea, Sean, et al. "Maintenance-Free Global Data Storage." *IEEE Internet Computing*, (Sep-Oct 2001). <a href="http://www.oceanstore.org/publications/papers/pdf/ieeeic.pdf">http://www.oceanstore.org/publications/papers/pdf/ieeeic.pdf</a>

Rose, Michael. "Hacked iCloud Password Leads to Nightmare." TUAW (2012-08-04). <a href="http://www.tuaw.com/2012/08/04/hacked-icloud-password-leads-to-nightmare/">http://www.tuaw.com/2012/08/04/hacked-icloud-password-leads-to-nightmare/</a>

Schwartzberg, David. "Cloud Storage Data Risks and Encryption." *nakedsecurity* (2012-08-03). <a href="http://nakedsecurity.sophos.com/2012/03/08/cloud-storage-data-risks-and-encryption/">http://nakedsecurity.sophos.com/2012/03/08/cloud-storage-data-risks-and-encryption/</a>

SSL. "What is SSL?" <a href="http://info.ssl.com/article.aspx?id=10241">http://info.ssl.com/article.aspx?id=10241</a>

Top 10 Cloud Storage. "The Importance of Data Encryption in Cloud Storage." (2012-11-16). <a href="http://www.top-10-cloud-storage.com/the-importance-of-data-encryption-in-cloud-storage/">http://www.top-10-cloud-storage.com/the-importance-of-data-encryption-in-cloud-storage/</a>

Ying, Jon. "Dropbox Around the World!" (2012-11-13). <a href="https://blog.Dropbox.com/?p=339">https://blog.Dropbox.com/?p=339</a>

Zelman, Josh. "How Dropbox got its First 10 million Users." *TechCrunch* (2011-11-01). <a href="http://techcrunch.com/2011/11/01/founder-storie-how-Dropbox-got-its-first-10-million-users/">http://techcrunch.com/2011/11/01/founder-storie-how-Dropbox-got-its-first-10-million-users/</a>

\* \* \*

#### **BIO**

Jeremy Legendre < <a href="mailto:jlegendre@stu.norwich.edu">mailto:jlegendre@stu.norwich.edu</a> is a currently entering his third year of studies in Norwich University's Bachelor of Science in Computer Security and Information Assurance (BSCSIA) program</a> <a href="mailto:http://programs.norwich.edu/business/csia/">http://programs.norwich.edu/business/csia/</a> > and hopes eventually to work with the US Department of Defense in cyber security. He has been programming since the age of thirteen and developed an antivirus for Mac OS X in the summer of 2012. He has always had a passion for technology and hopes to continue to an enjoyable and prosperous career in IT.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

# Think Before You Post: Adapting to a Changing Technological Environment

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University

I'm tired of hearing old people (half my age, even) moaning about changes in the standards and behaviour of younger people. We have a responsibility to our youngsters to help them avoid obvious pitfalls in the use of communications technology.

In February 2013, an 18 year-old online gaming enthusiast called Justin Carter responded to insulting remarks in a Facebook posting that questioned his sanity. He responded, "Oh yeah, I'm real messed up in the head, I'm going to go shoot up a school full of kids and eat their still, beating hearts. LOL JK"

Another Facebook user reported Carter to local police in his home town in Texas. Local police arrested him for "making a terroristic threat" and locked him up from February 14 until March 13, which is when he was first questioned about his comment. After posting a request for support< <a href="https://www.change.org/petitions/release-my-son-justin-carter-being-prosecuted-for-a-facebook-comment">https://www.change.org/petitions/release-my-son-justin-carter-being-prosecuted-for-a-facebook-comment</a> with the whole story and updates, his family has succeeded in having the young man released on bail (thanks to an anonymous donor of 10% of the \$500,000 bond)<<a href="http://www.readthehorn.com/blogs/talking-heads/81043/op-ed-protect-our-freedom-free-justing-neads-nead

As of this writing in July 2013, Carter is still due to be prosecuted. A search on his name using any Web search engine brings up a flood of hits.

I don't want to discuss the specifics of Carter's comments; there's plenty of thought-provoking commentary online already. What strikes me is the need to adapt our cultural norms to the reality of today's social networking.

As I have written elsewhere,< <a href="http://www.mekabay.com/ethics/totem\_taboo\_cyber.pdf">http://www.mekabay.com/ethics/totem\_taboo\_cyber.pdf</a> > we need to integrate cyberspace into our moral universe – and that applies in particular to helping children learn what are new rules for older adults but should be norms for children and young adults.</a><a href="http://www.networkworld.com/newsletters/2010/060710sec1.html">http://www.networkworld.com/newsletters/2010/060710sec1.html</a> >

In the Parkerian Hexad, < <a href="http://www.mekabay.com/overviews/hexad\_ppt.zip">http://www.mekabay.com/overviews/hexad\_ppt.zip</a> > the concept of control refers to how information can be shared, modified, sequestered or destroyed. The example I've used for years to distinguish between control and confidentiality is why we instantly recognize that if someone steals your new credit card in its sealed envelope from your mailbox – but doesn't open the envelope – they have not violated confidentiality. They still don't know your credit-card number. However, they do have the ability to do anything they want with your credit card. They can see it if they open the envelope, sell the number to the Russian Business Network, <a href="http://www.networkworld.com/newsletters/sec/2011/032811sec1.html">http://www.networkworld.com/newsletters/sec/2011/032811sec1.html</a> > or cut it up and throw away the pieces. They control the information.

Children must be taught that anything they put online is out of their control – forever. Not only

are there archives of now-deleted Webpages,< <a href="http://archive.org/web/web.php">http://archive.org/web/web.php</a> > but anyone can copy text, save pictures, or keep a screenshot of whatever has been emailed or posted online. Once digital information has been made accessible to others, the original owners can do nothing in practice to stop its spread.

Sexting,< <a href="http://www.networkworld.com/newsletters/sec/2011/072511sec2.html">http://www.networkworld.com/newsletters/sec/2011/072511sec2.html</a> or sending pornography (even child pornography) by the Short Message Service (SMS) to mobile devices, has led to embarrassment, humiliation, bullying (sometimes even unto suicide) and prosecutions for violations of child-pornography laws. If parents and teachers accept that teaching children to keep (most of) their clothes on in public (apologists to nudists – no offense intended), it seems sensible to expand the training (OK, indoctrination) to include not sending pictures of one's naked self to anyone else – at least, not until the age of legal majority.

Yes, the same could be said of conversations in the playground and papers left in a room at home – but most children don't use digital recorders and cameras as a matter of course (yet – just wait until children start wearing Google Glasses< <a href="http://www.google.com/glass/start/">http://www.google.com/glass/start/</a> > and future equivalents). We have to adapt to the reality of how computing and mobile communications have become central to young people's interactions.</a> <a href="http://www.ted.com/talks/john mcwhorter txtng">http://www.ted.com/talks/john mcwhorter txtng</a> is killing language jk.html >

So instead of futilely bemoaning changes in cultural styles of communication as if anything younger people do must inherently be wrong,< <a href="http://ideas.time.com/2013/04/25/is-texting-killing-the-english-language/">http://ideas.time.com/2013/04/25/is-texting-killing-the-english-language/</a> we need collectively to adapt to reality (REALITY TRUMPS THEORY). Starting in infancy, children need to be taught over and over, in every possible way, to use their communications technology well and safely. Elementary schools — kindergarten — should be integrating cyberspace into the curriculum. Middle and high schools would do well to include explicit discussions about bizarre behaviour such as posting terroristic jokes on social networks and sending auto-pornographic photos to other teenagers (remember, the frontal lobes, responsible for rationality, are underdeveloped until the late teens or early twenties</a> <a href="http://www.hhs.gov/opa/familylife/tech\_assistance/etraining/adolescent\_brain/Development/prefrontal\_cortex/">http://www.hhs.gov/opa/familylife/tech\_assistance/etraining/adolescent\_brain/Development/prefrontal\_cortex/</a>). Colleges and universities must expand their ethics training to cope with the realities of today's technological and social environments.

Let's get on with it, folks: we've *got* to help youngsters learn how to be safe online.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:mekabay@gmail.com">http://www.mekabay.com/</a> >

\* \* \*

Copyright © 2013 M. E. Kabay. All rights reserved.

# Updates to Chapter on Privacy in Cyberspace (1): US Domestic Spying & UK Phone-Hacking Scandal

M. E. Kabay, PhD, CISSP-ISSMP

I just completed another marathon editing task, working on updating a chapter about privacy that had not been updated since 2008. Here are some new sections that may interest readers.

\* \* \*

As this chapter was going to press in July 2013, cyber-privacy issues in the US and Europe were actively being covered by the news media and generating concern among civil liberties groups. The domestic spying programs of the US National Security Agency and questions about illegal phone tapping in the United Kingdom were top news items.

Several cases have caused interest among privacy advocates in the first decades of the 21<sup>st</sup> century.

## **NSA Domestic Spying**

The Electronic Frontier Foundation (EFF) page about extra-legal surveillance of US residents includes this succinct summary:

In October 2001, President Bush issued a secret presidential order authorizing the NSA to conduct a range of surveillance activities inside of the United States without statutory authorization or court approval, including electronic surveillance of Americans' telephone and Internet communications. This program of surveillance continues through today, although the legal justifications have changed over time, and works with the major telecommunications and Internet companies.

In 2005, after the New York Times broke the story of the surveillance program, the President publicly admitted one portion of it—warrantless surveillance of Americans believed to be communicating with people connected with terrorism suspects—Senior Bush Administration officials later confirmed that the President's authorization went beyond the surveillance of terrorists and conceded that the program did not comply with the Foreign Intelligence Surveillance Act (FISA). The President, invoking a theory of limitless executive power to disregard the mandates of Congress, reauthorized this warrantless surveillance more than thirty times, including after the Department of Justice found the program to violate criminal laws. President Obama has continued the program, but with differing secret legal justifications. Obama has given no public legal justification for it and, in some situations, appears to be strategically denying certain portions of it. For other portions, including the collection of telecommunications records, the Obama Administration said it could neither confirm nor deny its actions until May, 2013, when the DNI finally admitted additional portions of it. Members of Congress have confirmed that additional domestic surveillance by the NSA still remains a secret.[1]

#### **NSA PRISM in US**

In July 2013, the Electronic Privacy Information Center (EPIC) reported on its efforts to block the widespread collection of call detail records (metadata) about phone calls originating or terminating in the US:

EPIC has filed a petition with the US Supreme Court, asking the Court to vacate an unlawful order by the Foreign Intelligence Surveillance Court that enables the NSA's collection of all domestic

phone records. On April 25, the secret court ordered Verizon to turn over all "call detail records" for calls made "wholly within the United States, including local telephone calls."

The FISC's order is based on Section 215 of the USA PATRIOT Act, which allows the court to compel the disclosure of business records that are "relevant to an authorized investigation." The Verizon order, however, requires the disclosure of all telephone records in the company's database.

"It is simply not possible that every phone record in the possession of a telecommunications firm could be relevant to an authorized investigation," EPIC states. "Such an interpretation of [the law] would render meaningless the qualifying phrases contained in the provision and eviscerate the purpose of the Act. "To define the scope of the records sought as 'everything' nullifies the relevance limitation in the statute," EPIC continues. "If law enforcement has 'everything,' there will always be some subset of 'everything' that is relevant to something."

The call detail records provided to the NSA, called "telephony metadata," contain an immense amount of sensitive personal information. The records identify the phone numbers of both parties on a call, the call's time and duration, and the geographic location of each phone number. When aggregated, such records can map out "the daily activities, interactions, personal and business relationships, religious and political affiliations, and other intimate details of millions of Americans," says EPIC.

EPIC's petition asks the Supreme Court to issue a "writ of mandamus" vacating the Verizon Order issued by the FISC. Mandamus is a command from a higher court to a lower court or government official, used when a lower court extends beyond the scope of its legal authority. EPIC writes, "Mandamus relief is warranted because the FISC exceeded its statutory jurisdiction when it ordered the production of millions of domestic telephone records that cannot plausibly be relevant to an authorized investigation."

EPIC brought the petition directly to the Supreme Court because no other court has jurisdiction to address the unlawful order. The Foreign Intelligence Surveillance Act (FISA) allows only the government and the recipient of a production order (i.e. Verizon) to appear before the FISC or the Court of Review. Additionally, the law limits these courts to hearing only certain types of appeals. EPIC, a Verizon customer whose call records are subject to the order, would not be able to obtain relief from these courts.[2]

## **Phone Hacking in UK**

*The Telegraph* provides a detailed timeline of the events known as the UK phone-hacking scandal.[3] Key events include

- 2005-11: The Royal Family complains about interception of private voicemail messages revealing a knee injury to Prince William.
- 2006-08: "Detectives arrest the *News of the World*'s royal editor Clive Goodman and private investigator Glenn Mulcaire over allegations that they hacked into the mobile phones of members of the royal household."
- 2007-01: "The *News of the World's* royal affairs editor Clive Goodman is jailed for four months. Private investigator Glenn Mulcaire is given a six-month prison term. Goodman and Mulcaire admitted conspiring to intercept communications while Mulcaire also pleaded guilty to five other charges of intercepting voicemail messages."
- 2009-07: "It emerges that News of the World reporters, with the knowledge of senior staff, illegally accessed messages from the mobile phones of celebrities and politicians while Coulson was editor from 2003 to 2007. It is also reported that News Group Newspapers, which publishes the News of the World, has paid out more than £1 million

- to settle cases that threatened to reveal evidence of its journalists' alleged involvement in phone hacking."
- 2011-01: "British police open a new investigation into allegations of phone hacking at the tabloid called 'Operation Weeting' after actress Sienna Miller, MP George Galloway and RMT union leader Bob Crow claim their phones were hacked."
- 2011-02: "The Met Police release a statement saying officers have identified more
  potential victims of hacking while reviewing files relating to the original Goodman and
  Mulcaire case. They say they are urgently notifying people who had previously been told
  that police had "little or no information" about them.
- Former Deputy Prime Minister Lord Prescott, Labour MP Chris Bryant, ex-Scotland Yard commander Brian Paddick and journalist Brendan Montague, all alleged victims of phone hacking, win a High Court bid for a judicial review into the police inquiry. They believe their human rights were breached.
- Lawyers for a football agent suing the *News of the World* claim Glenn Mulcaire passed information directly to the newsdesk rather than an individual reporter, Goodman. They say the desk could have been staffed by "a number of journalists", and suggest that this means knowledge of phone-hacking was more widespread than previously admitted. A judge rules that Mulcaire must provide information about whether other journalists at the NoW were involved in hacking. He had tried to claim he should be exempt from giving evidence for fear of incriminating himself."
- 2011-03: "The BBC's Panorama reveals that in 2006, a then *News of the World* executive, Alex Marunchak, obtained e-mails belonging to an ex-British Army intelligence officer that had been hacked in to by a private detective."
- 2011-04: "Former *News of the World* editor Ian Edmondson, chief reporter Neville Thurlbeck and senior journalist James Weatherup are arrested on suspicion of conspiring to intercept mobile phone messages. They are released on bail until September. The *News of the World* admits it had a role in phone hacking. The *News of the World* publishes apologies on both its website and newspaper. News International also announces it will set up a compensation scheme to deal with "justifiable claims" fairly and efficiently. However, the publisher adds it will continue to contest cases "that we believe are without merit or where we are not responsible."
- 2011-05: "Former Deputy Prime Minister Lord Prescott, Labour MP Chris Bryant, ex-Scotland Yard commander Brian Paddick and journalist Brendan Montague, all alleged victims of phone hacking, win a High Court bid for a judicial review into the police inquiry. They believe their human rights were breached."

In November 2012, Lord Justice Leveson released his report on the scandal.[4] Some of the key findings in the *Executive Summary* follow:

- "The evidence placed before the Inquiry has demonstrated, beyond any doubt, that there have been far too many occasions over the last decade and more (itself said to have been better than previous decades) when these responsibilities, on which the public so heavily rely, have simply been ignored. There have been too many times when, chasing the story, parts of the press have acted as if its own code, which it wrote, simply did not exist. This has caused real hardship and, on occasion, wreaked havoc with the lives of innocent people whose rights and liberties have been disdained. This is not just the famous but ordinary members of the public, caught up in events (many of them, truly tragic) far larger than they could cope with but made much, much worse by press behaviour that, at times, can only be described as outrageous."
- "For many years, there have been complaints that certain parts of the press ride roughshod over others, both individuals and the public at large, without any justifiable

- public interest. Attempts to take them to task have not been successful. Promises follow other promises. Even changes made following the death of Diana, Princess of Wales, have hardly been enduring. Practices discovered by the Information Commissioner, during Operation Motorman, which led to the publication of two reports to Parliament,8 revealed that large parts of the press had been engaged in a widespread trade in private and confidential information, apparently with little regard to the public interest. A private detective, Steve Whittamore, had certainly been engaged in wholesale criminal breaches of data protection legislation and, prima facie, journalists who engaged his services or used his products (and paid substantial sums for the privilege) must or should have appreciated that the information could not have been obtained lawfully."
- "When Clive Goodman, a journalist employed by the News of the World and Glenn Mulcaire, a private detective, were convicted of hacking into the telephone messages of members of the Royal Household and others, it was implicit during the course of the criminal prosecution that others must have been involved, whether knowingly or not, in using information that was the product of phone hacking. Most responsible corporate entities would be appalled that employees were or could be involved in the commission of crime in order to further their business. Not so at the News of the World. When the police had sought to execute a warrant, they were confronted and driven off by the staff at the newspaper. Cooperation, if provided, was minimal. The two that were sentenced to terms of imprisonment were paid very substantial sums as compensation for loss of employment when they were released."
- Then came exposure of the fact, albeit as long ago as March 2002, that the mobile phone of Milly Dowler had been hacked by someone at the News of the World. The information obtained had led the paper to publish false leads as a result of its misunderstanding of a message which had simply been left on the wrong phone in error. It was also believed that a message or messages had been deleted (thereby giving rise to a false moment of hope in her family). On 5 July 2011, these facts were reported by the Guardian. The outcry was immediate; Two days later it was announced that the News of the World would close."
- "Phone hacking in itself, even if it were only in one title, would justify a reconsideration of the corporate governance surrounding the way in which newspapers operate and the regulatory regime that is required. Without making findings against anyone individually, the evidence drives me to conclude that this was far more than a covert, secret activity, known to nobody save one or two practitioners of the 'dark arts'. Yet it was illegal. And after the prosecution, at more than one title and more than one publisher, there was no indepth look to examine who had been paid for what and why or to review compliance requirements."

#### **ENDNOTES**

- "What is the NSA domestic spying program?" NSA Spying on Americans, Electronic Frontier Foundation (2013-07-31). <a href="https://www.eff.org/nsa-spying/faq#37">https://www.eff.org/nsa-spying/faq#37</a>
- [2] "EPIC Urges US Supreme Court to Suspend NSA Domestic Surveillance." EPIC Alert 20.14 (2013-07-12). http://epic.org/alert/epic\_alert\_20.14.html
- [3] Chandrasekhar, M. Wardrop and A. Trotman. "Phone hacking: timeline of the scandal: The key events in the phone hacking scandal, which has led to the closure of the News of the World, halted Rupert Murdoch's BSkyB takeover bid, and prompted the arrest of several key figures." *The Telegraph* (2012-07-23). <a href="http://www.telegraph.co.uk/news/uknews/phone-hacking/8634176/Phone-hacking-timeline-of-a-scandal.html">http://www.telegraph.co.uk/news/uknews/phone-hacking/8634176/Phone-hacking-timeline-of-a-scandal.html</a>
- [4] Lord Justice Leveson. *An Inquiry into the Culture, Practices and Ethics of the Press:*Executive Summary. <a href="http://media.ft.com/cms/643fca7e-3a2c-11e2-a00d-00144feabdc0.pdf">http://media.ft.com/cms/643fca7e-3a2c-11e2-a00d-00144feabdc0.pdf</a>

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:mekabay@gmail.com">http://www.mekabay.com/</a> >

## Updates to Chapter on Privacy in Cyberspace (2): Developments in Australia & Europe

#### M. E. Kabay, PhD, CISSP-ISSMP

Here's some more new material I just added in another marathon editing task, working on updating a chapter about privacy that had not been updated since 2008.

\* \* \*

The Office of the Privacy Commissioner of Australia summarizes the emerging principles for privacy protection as its *National Privacy Principles* (NPPs), as follows (quoting directly):

- NPP 1: collection. Describes what an organisation should do when collecting
  personal information, including what they can collect, collecting from third parties
  and, generally, what they should tell individuals about the collection.
- NPP 2: use and disclosure. Outlines how organisations may use and disclose individuals' personal information. If certain conditions are met, an organisation does not always need an individual's consent to use and disclose personal information. There are also rules about direct marketing.
- NPPs 3–4: information quality and security. An organisation must take steps to ensure the personal information it holds is accurate and up-to-date, and is kept secure from unauthorised use or access.
- NPP 5: openness. An organisation must have a policy on how it manages personal information, and make it available to anyone who asks for it.
- NPP 6: access and correction. Gives individuals a general right of access to their personal information, and the right to have that information corrected if it is inaccurate, incomplete or out-of-date.
- NPP 7: identifiers. Generally prevents an organisation from adopting an Australian Government identifier for an individual (eg Medicare numbers) as its own.
- NPP 8: anonymity. Where possible, organisations must give individuals the
  opportunity to do business with them without the individual having to identify
  themselves.
- NPP 9: transborder data flows. Outlines how organisations should protect personal information that they transfer outside Australia.
- NPP 10: sensitive information: Sensitive information includes information relating to health, racial or ethnic background, or criminal records. Higher standards apply to the handling of sensitive information.[5]

## State of Implementation of the EU Privacy Directive

As of July 2013, the 28 member countries of the European Union, including the new members states, have passed legislation fully implementing the Privacy Directive.[6]

In January 2012, the EU received a plan for improving privacy protection:

The European Commission has ... proposed a comprehensive reform of the EU's 1995 data protection rules to strengthen online privacy rights and boost Europe's digital economy. Technological progress and globalisation have profoundly changed the way our data is collected, accessed and used. In addition, the 27 EU Member States have implemented the 1995 rules differently, resulting in divergences in enforcement. A single law will do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year. The initiative will help reinforce consumer confidence in online services, providing a much needed boost to growth, jobs and innovation in Europe.[7]

According to a press release,

Key changes in the reform include:

- A single set of rules on data protection, valid across the EU. Unnecessary administrative requirements, such as notification requirements for companies, will be removed. This will save businesses around €2.3 billion a year.
- Instead of the current obligation of all companies to notify all data protection activities to data protection supervisors − a requirement that has led to unnecessary paperwork and costs businesses €130 million per year, the Regulation provides for increased responsibility and accountability for those processing personal data.
- For example, companies and organisations must notify the national supervisory authority of serious data breaches as soon as possible (if feasible within 24 hours).
- Organisations will only have to deal with a single national data protection authority in the EU country where they have their main establishment. Likewise, people can refer to the data protection authority in their country, even when their data is processed by a company based outside the EU. Wherever consent is required for data to be processed, it is clarified that it has to be given explicitly, rather than assumed.
- People will have easier access to their own data and be able to transfer personal data from one service provider to another more easily (right to data portability).
   This will improve competition among services.
- A 'right to be forgotten' will help people better manage data protection risks online: people will be able to delete their data if there are no legitimate grounds for retaining it.
- EU rules must apply if personal data is handled abroad by companies that are active in the EU market and offer their services to EU citizens.
- Independent national data protection authorities will be strengthened so they can better enforce the EU rules at home. They will be empowered to fine companies that violate EU data protection rules. This can lead to penalties of up to €1 million or up to 2% of the global annual turnover of a company.
- A new Directive will apply general data protection principles and rules for police and judicial cooperation in criminal matters. The rules will apply to both domestic and cross-border transfers of data.[8]

Readers committed to following the Directive will want to keep tabs on developments as these proposals wend their way through the EU deliberative process.

## **Establishment of the European Data Protection Supervisor**

In 2002, the European Parliament and the European Council established the office of the European Data Protection Supervisor (EDPS), described as follows:

The EDPS is an independent supervisory authority devoted to protecting personal data and privacy and promoting good practice in the EU institutions and bodies. He does so by:

- monitoring the EU administration's processing of personal data;
- advising on policies and legislation that affect privacy; and
- cooperating with similar authorities to ensure consistent data protection....

The supervisory task is to ensure that the EU institutions and bodies process personal data of EU staff and others lawfully. The EDPS oversees Regulation (EC) 45/2001 on data protection, which is based on two main principles:

The responsible data controller needs to respect a number of obligations. For instance, personal data can only be processed for a specific and legitimate reason which must be stated when the data are collected.

The person whose data are processed - the data subject - enjoys a number of enforceable rights. This includes, for instance, the right to be informed about the processing and the right to correct data.

Every institution or body should have an internal Data Protection Officer. The DPO keeps a register of processing operations and notifies systems with specific risks to the EDPS. The EDPS prior checks whether or not those systems comply with data protection requirements. The EDPS also deals with complaints and conducts inquiries.[9]

In July 2013, the EDPS issued a report strongly criticizing the European Commission's plans for implementing computer-assisted border checks (*smart borders*). Peter Hustinx, the Director of the EDPS, was quoted as saying,

"In the absence of such a policy, the creation of yet another large-scale IT database to store massive amounts of personal information is a disproportionate response to a problem that other recently created systems may be able to help solve. It would be prudent both economically and practically to evaluate the existing systems at least to ensure consistency and best practice." [10]

On July 31, 2013, the positions of EDPS and Assistant Supervisor became vacant.[11] It was not known whether there was a relationship between the EDPS criticism of smart borders and the vacancy.

## **ENDNOTES**

[5] According to the Australian Government, "The Privacy Amendment Act includes a set of new, harmonised, privacy principles that will regulate the handling of personal information by both Australian government agencies and businesses. These new principles are called the Australian Privacy Principles (APPs). They will replace the existing Information Privacy Principles (IPPs) that currently apply to Australian

- government agencies and the National Privacy Principles (NPPs) that currently apply to businesses.
- [6] Under the changes, there will be 13 new APPs. A number of the APPs are significantly different from the existing principles, including APP 7 on the use and disclosure of personal information for direct marketing, and APP 8 on cross-border disclosure of personal information." See <a href="http://www.oaic.gov.au/privacy/privacy-act/privacy-law-reform/what-s-changed">http://www.oaic.gov.au/privacy/privacy-act/privacy-law-reform/what-s-changed</a>
- "Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data." European Commission (2013-07-16). http://ec.europa.eu/justice/data-protection/law/status-implementation/index\_en.htm
- [8] "Commission proposes a comprehensive reform of the data protection rules." European Commission (2012-01-25). <a href="http://ec.europa.eu/justice/newsroom/data-protection/news/120125\_en.htm">http://ec.europa.eu/justice/newsroom/data-protection/news/120125\_en.htm</a>
- [9] "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses." EUROPA Press Releases (2012-01-25). <a href="http://europa.eu/rapid/press-release\_IP-12-46\_en.htm">http://europa.eu/rapid/press-release\_IP-12-46\_en.htm</a>
- [10] European Data Protection Supervisor. https://secure.edps.europa.eu/EDPSWEB/edps/EDPS
- [11] "EU Data Protection Supervisor slams 'smart borders'." NewEurope Online (2013-07-19). <a href="http://www.neurope.eu/article/eu-data-protection-supervisor-slams-smart-borders">http://www.neurope.eu/article/eu-data-protection-supervisor-slams-smart-borders</a>

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:mekabay@gmail.com">http://www.mekabay.com/</a> >

## **Updates to Chapter on Privacy in Cyberspace (3): FISA, FISC, USAPATRIOT, Libraries**

M. E. Kabay, PhD, CISSP-ISSMP

Here's yet more new material I just added in another marathon editing task, working on updating a chapter about privacy that had not been updated since 2008.

## Foreign Intelligence Surveillance Act and Court

The Foreign Intelligence Surveillance Court (FISC) was established in 1978 as part of the Foreign Intelligence Surveillance Act (FISA). The Federal Judicial Center of the US government describes the origin and functioning of FISC and FISA as follows:

Congress in 1978 established the Foreign Intelligence Surveillance Court as a special court and authorized the Chief Justice of the United States to designate seven federal district court judges to review applications for warrants related to national security investigations. Judges serve for staggered, non-renewable terms of no more than seven years, and until 2001 were drawn from different judicial circuits. The provisions for the court were part of the Foreign Intelligence Surveillance Act (92 Stat. 1783), which required the government, before it commenced certain kinds of intelligence gathering operations within the United States, to obtain a judicial warrant similar to that required in criminal investigations. The legislation was a response to a report of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the "Church Committee"), which detailed allegations of executive branch abuses of its authority to conduct domestic electronic surveillance in the interest of national security. Congress also was responding to the Supreme Court's suggestion in a 1972 case that under the Fourth Amendment some kind of judicial warrant might be required to conduct national security related investigations.

Warrant applications under the Foreign Intelligence Surveillance Act are drafted by attorneys in the General Counsel's Office at the National Security Agency at the request of an officer of one of the federal intelligence agencies. Each application must contain the Attorney General's certification that the target of the proposed surveillance is either a "foreign power" or "the agent of a foreign power" and, in the case of a U.S. citizen or resident alien, that the target may be involved in the commission of a crime.

The judges of the Foreign Intelligence Surveillance Court travel to Washington, D.C., to hear warrant applications on a rotating basis. To ensure that the court can convene on short notice, at least one of the judges is required to be a member of the U.S. District Court for the District of Columbia. The act of 1978 also established a Foreign Intelligence Surveillance Court of Review, presided over by three district or appeals court judges designated by the Chief Justice, to review, at the government's request, the decisions of the Foreign Intelligence Surveillance Court. Because of the almost perfect record of the Department of Justice in obtaining the surveillance warrants and other powers it requested from the Foreign Intelligence Surveillance Court, the review court had no occasion to meet until 2002. The USA Patriot Act of 2001 (115 Stat. 272) expanded the time periods for which the Foreign Intelligence Surveillance Court can authorize surveillance and increased the number of judges serving the court from seven to eleven. The eleven judges must be drawn from at least seven judicial circuits, and no fewer than three are to reside within twenty miles of the District of Columbia.[12]

In response to severe criticism by civil-liberties proponents, additional legislation was passed in 2007 and 2008 to strengthen the Executive Branch's powers to order wide-reaching surveillance without prior approval of the FISC.[13]

#### **USAPATRIOT Act**

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USAPATRIOT) Act, whose name was crafted to result in the positive-sounding acronym, was passed with minimal legislative review in October 2001 as a reaction to the terrorist attacks of September 11, 2001.[14]

The Electronic Frontier Foundation, a civil-liberties organization, summarizes its perception of the threats in the USAPATRIOT Act to online civil liberties as follows:

- The law dramatically expands the ability of states and the Federal Government to conduct surveillance of American citizens. The Government can monitor an individual's web surfing records, use roving wiretaps to monitor phone calls made by individuals "proximate" to the primary person being tapped, access Internet Service Provider records, and monitor the private records of people involved in legitimate protests.
- PATRIOT is not limited to terrorism. The Government can add samples to DNA
  databases for individuals convicted of "any crime of violence." Government spying
  on suspected computer trespassers (not just terrorist suspects) requires no court
  order. Wiretaps are now allowed for any suspected violation of the Computer Fraud
  and Abuse Act, offering possibilities for Government spying on any computer user.
- Foreign and domestic intelligence agencies can more easily spy on Americans.
   Powers under the existing Foreign Intelligence Surveillance Act (FISA) have been broadened to allow for increased surveillance opportunities. FISA standards are lower than the constitutional standard applied by the courts in regular investigations.
   PATRIOT partially repeals legislation enacted in the 1970s that prohibited pervasive surveillance of Americans.
- PATRIOT eliminates Government accountability. While PATRIOT freely eliminates
  privacy rights for individual Americans, it creates more secrecy for Government
  activities, making it extremely difficult to know about actions the Government is
  taking.
- PATRIOT authorizes the use of "sneak and peek" search warrants in connection with
  any federal crime, including misdemeanors. A "sneak and peek" warrant authorizes
  law enforcement officers to enter private premises without the occupant's permission
  or knowledge and without informing the occupant that such a search was conducted.
- The Department of Justice, with little input from Congress and the American people, is developing follow-on legislation the Domestic Security Enhancement Act (nicknamed Patriot II) -- which would greatly expand PATRIOT's already sweeping powers.[15]

The law firm of Kelly/Warner has published an excellent summary of the COPPA provisions.[16]

## **Privacy of Activity in Libraries and Bookshops**

In sharp contrast with the privacy provisions of privacy protections for cable television and video rentals and sales discussed in previous sections of this chapter, the USAPATRIOT Act specifically allows intelligence and law enforcement agencies to monitor the use of libraries and booksellers by patrons. Specifically, librarians are required to submit detailed borrowing records on demand and may not reveal that these records were surrendered.

The Patriot Act permits federal agents to secretly obtain information from booksellers and librarians about customers' and patrons' reading, internet and book-buying habits, merely by alleging that the records are relevant to an anti-terrorism investigation. The act prohibits librarians and booksellers from revealing these requests, so they cannot be challenged in court.... A University of Illinois study ... concludes that federal agents have sought records from about 220 libraries nationwide since September 2001... [as of January 2002]. The Justice Department refuses to say how many times it has invoked this Patriot Act provision ... But Assistant Attorney General Daniel Bryant says that people who borrow or buy books surrender their right of privacy.... Some libraries and bookstores unhappy with the law begin to fight back in a number of ways. Some libraries have posted signs warning that the government may be monitoring their users' reading habits.... Thousands of libraries are destroying records so agents have nothing to seize.... Many librarians polled say they would break the law and deny orders to disclose reading records.[17]

The American Library Association explains their perspective on why the provisions matter to the public:

Libraries are key sources of information on all kinds of subjects and from all perspectives for their communities. Reading has always been one of our greatest freedoms. The written word is the natural medium for the new idea and the untried voice from which come the original contributions to social growth.

Libraries provide a place to exercise intellectual freedom: a free and open exchange of knowledge and information where individuals may exercise freedom of inquiry as well as a right to privacy in regards to information they seek. Privacy is essential to the exercise of free speech, free thought, and free association. In a library, the subject of users' interests should not be examined or scrutinized by others.

The ALA believes certain sections of the USA PATRIOT Act endanger constitutional rights and privacy rights of library users. Libraries cooperate with law enforcement when presented with a lawful court order to obtain specific information about specific patrons; however, the library profession is concerned some provisions in the USA PATRIOT Act go beyond the traditional methods of seeking information from libraries.[18]

#### **ENDNOTES**

- [12] <a href="http://www.fjc.gov/history/home.nsf/page/courts\_special\_fisc.html">http://www.fjc.gov/history/home.nsf/page/courts\_special\_fisc.html</a>
- [13] "Beyond FISA." Electronic Frontier Foundation (2013). https://ssd.eff.org/foreign/beyond-fisa
- [14] "The USA PATRIOT Act." Electronic Frontier Foundation (2005-08-03). http://w2.eff.org/patriot/
- [15] "How PATRIOT Threatens Online Civil Liberties." Electronic Frontier Foundation (2013). http://w2.eff.org/patriot/why.php
- [16] Kelly/Warner Internet Law & Defamation Practice. "COPPA: Children's Online Privacy Protection Act Summary." (2012). <a href="http://www.aaronkellylaw.com/coppa-childrens-online-privacy-protection-act-summary/">http://www.aaronkellylaw.com/coppa-childrens-online-privacy-protection-act-summary/</a>
- [17] "January 2002: Study Finds Agents Have Sought Records From 220 Libraries." Profile: USA Patriot Act, History Commons (2002). http://www.historycommons.org/entity.jsp?entity=patriot\_act
- [18] "The USA PATRIOT Act." American Library Association (2013). http://www.ala.org/advocacy/advleg/federallegislation/theusapatriotact

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<
a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

## **Updates to Chapter on Privacy in Cyberspace (4): Cookies, Glasses, Readings**

M. E. Kabay, PhD, CISSP-ISSMP

Here's yet more new material I just added in another marathon editing task, working on updating a chapter about privacy that had not been updated since 2008.

#### **COOKIES**

Cookies are small files stored on a user's computer so that a Web server can access information such as identity, browsing history, preferences, and so on.

The Electronic Privacy Information Center (EPIC) has a long history of what it defines as abuse of cookies:

EPIC filed a complaint ... with the Federal Trade Commission on February 10, 2000, concerning the information collection practices of DoubleClick Inc., a leading Internet advertising firm, and its business partners. The complaint alleges that DoubleClick is unlawfully tracking the online activities of Internet users (through the placement of cookies) and combining surfing records with detailed personal profiles contained in a national marketing database. EPIC's complaint follows the merger of DoubleClick and Abacus Direct, the country's largest catalog database firm. DoubleClick has announced its intention to combine anonymous Internet profiles in the DoubleClick database with the personal information contained in the Abacus database.[19]

For extensive resources about legal aspects of Web cookies, see the EPIC *Cookies* Web page.[19]

#### **GOOGLE GLASSES**

A technology that was garnering a great deal of media attention as this chapter was going to press in July 2013 was the *Google Glass*, a wearable, networked computer that includes a camera and projects information in the user's field of view. The device can not only record information from the user's environment, it can provide information about recognized people in the field of view.[20]

Great concern has been expressed by privacy advocates that information about individuals' every move will become available before any clear rules are established concerning the protection or use of that information. For example, EPIC writes,

When individuals are moving about in public and private spaces, they do not expect to be tracked wherever they go. However, this expectation is being challenged as cell phones and other electronic devices now collect and store location data throughout the day. The expansion of location tracking technologies has significant implications for consumers and for their constitutional privacy rights.

Over the last 10 years, law enforcement has stepped up its use of location tracking technologies, such as GPS (Global Positioning System) trackers and cell phones, to

monitor the movements of individuals who may or may not be suspected of a crime. GPS is a geolocation network that consists of satellites and receivers that can calculate the precise location of a GPS device 24-hours a day (subject to environmental constraints). As of March 19, 2013, there are 31 satellites in the GPS constellation. The satellites and ground stations in the GPS network are maintained by the U.S. Air Force Global Positioning Systems Wing. GPS satellites are designed to transmit three-dimensional location data (longitude, latitude and altitude) as well as precise velocity and timing information to an unlimited number of users simultaneously. A GPS receiver is all that one needs to access the service. GPS satellites can not receive any data, they can only broadcast location and timing information.[21]

## **Further Reading**

Bennett, C. J. and C. D. Raab. *The Governance of Privacy: Policy Instruments in a Global Perspective*. MIT Press, 2006.

Bygrave, L. A. Data Protection Law: Approaching Its Rationale, Logic and Limits. Kluwer Law International, 2002.

Harvey, I., A. Cavoukian, G. Tomko, D. Borrett, H. Kwan, and D. Hatzinakos, editors. *SmartData: Privacy Meets Evolutionary Robotics*. Springer, 2013.

Hoepman, J.-H. and I. Verbauwhede, editors. *Radio Frequency Identification: Security and Privacy Issues: 8th International Workshop, RFIDSec 2012, Nijmegen, The Netherlands, July 2-3, 2012.* Springer, 2013.

Nehf, J. P. *Open Book: The Failed Promise of Information Privacy in America*. CreateSpace Independent Publishing Platform, 2012.

Rosen, J. and B. Wittes, editors. *Constitution 3.0: Freedom and Technological Change*. Brookings Institution Press, 2013.

Solove, D. J., M. Rotenberg, and P. J. Schwartz. *Information Privacy Law*. Aspen, 2006.

Solove, D. J. *Understanding Privacy*. Harvard University Press, 2010.

Solove, D. J. Nothing to Hide: The False Tradeoff between Privacy and Security. Yale University Press, 2013.

Stewart, D., editor. Social Media and the Law: A Guidebook for Communication Students and Professionals. Routledge, 2012.

Ziegler, K. S. Human Rights and Private Law: Privacy as Autonomy. Hart, 2007.

#### **WEB SITES**

- American Civil Liberties Union: http://www.aclu.org/
- Electronic Privacy Information Center: <a href="http://epic.org">http://epic.org</a>
- European Commission, Justice and Home Affairs, Data Protection: http://ec.europa.eu/justice/data-protection/index\_en.htm
- Federal Trade Commission, Privacy Initiatives: <a href="http://business.ftc.gov/privacy-and-security">http://business.ftc.gov/privacy-and-security</a>
- National Conference of State Legislatures, NCSL 50—State Legislative Tracking Resources: http://www.ncsl.org/legislative-staff.aspx?tabs=856,34,736

- Privacy, Business and Law—Pandab is an online newsletter summarizing the top news articles on privacy, law and business: http://www.pandab.org
- Privacy Exchange—a global information resource on consumers, commerce, and date protection worldwide: <a href="http://www.privacyexchange.org">http://www.privacyexchange.org</a>
- Privacy International—Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations: <a href="http://www.privacyinternational.org">http://www.privacyinternational.org</a>

#### **ENDNOTES**

- [19] "EPIC Files FTC Privacy Complaint Against DoubleClick." Cookies, Electronic Privacy Information Center. <a href="http://epic.org/privacy/internet/cookies/">http://epic.org/privacy/internet/cookies/</a>
- [20] "Google Glass may compromise privacy of user and others." KTVU TV (2013-05-16). http://www.ktvu.com/news/news/special-reports/google-glass-may-compromise-privacy-user-and-other/nXtHx/
- [21] Locational Privacy. Electronic Privacy Information Center. <a href="http://epic.org/privacy/location\_privacy/">http://epic.org/privacy/location\_privacy/</a>

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

## Being Dr Evil for a Moment

by M. E. Kabay, PhD, CISSP-ISSMP Professor of Computer Information Systems School of Business & Management Norwich University, Northfield VT

Friend and colleague Prof Ric Steinberger < <a href="http://www.linkedin.com/pub/ric-steinberger/15/677/106">http://www.linkedin.com/pub/ric-steinberger/15/677/106</a> > wrote the following thoughtful essay in one of his email messages and has granted permission to post it here. Everything below is Ric's own work with minor edits from Mich.

\* \* \*

Most people who work in information security are accustomed to thinking defensively: How can I prevent "bad things" from happening that would damage computers or networks, or allow unauthorized people to view/alter confidential information? We seldom are in a position to think offensively: How would I attack or damage an opponent's systems or gain access to information the opponent doesn't want me to see?

Edward Snowden's recent releases – mostly through Glenn Greenwald of *The Guardian* < <a href="http://www.theguardian.com/world/nsa">http://www.theguardian.com/world/nsa</a> > – make it clear that the NSA is very much playing offense – trying really hard to obtain copies of every bit of digital information that US citizens (and those of many other nations) have created. As documented in extensive references by the Electronic Frontier Foundation < <a href="https://www.eff.org/nsa-spying">https://www.eff.org/nsa-spying</a> >, the NSA gets copies of all phone calls (metadata, and probably call content), emails, files in the cloud, communications on social networks like Facebook, copies of physical letter envelopes. Several large US based companies have been corralled into this effort, named Prism: Yahoo, Microsoft, Apple, Google, AOL, Facebook, Twitter, Paltalk, perhaps more that have not been revealed so far.

But what does the NSA not have access to unless the FBI physically plants some kind of device or software bug on their targets' computers and networks? [Note that the NSA targets are all US citizens plus many in other nations.] As far as we know, the NSA cannot do direct searches or copies of individuals' computer systems, home or business networks. Why not? Because in many cases, users may create this data without its ever being transmitted over the Internet. Could the NSA break into specific systems physically and/or electronically? Of course. But that requires time, manpower, money and in theory, a warrant issued by a judge. Therefore imagine plotters in different locations collaborating by creating local information, copying it to USB thumb drives and mailing them to each other. Do we really imagine that the NSA has not considered this?

So, if I were director of strategy at the NSA, I would want unfettered, universal access to that "last mile," the final refuge of Americans' digital privacy: files stored on their personal computers, including smart phones. The question is: How do I get it? I can't have the FBI break into every house and business in the country, at least not yet. But what if I could install spyware and/or botnet clients on every major operating system? OK, how do I do that? There are a couple approaches, each with advantages and disadvantages. I could try to bully Microsoft, Google, Apple and some Linux vendors into installing the spyware/botnet software via patches. Most of these companies are already part of Prism, so in theory, I could just extend the "Prism walls." But what if that's just too obvious? What if the Prism companies successfully push

back, or tie me down for years with legal challenges?

So I move to plan B: I approach the major US anti-malware companies, like Symantec, McAfee, ESET, more. Anti-malware software is installed on almost every home and work PC/Mac computer. I get National Security Letters and force these companies into the Prism program. Then I require them to add a high quality (think Stuxnet) spyware/botnet client that is capable of reporting on and even sending copies of every file a user possesses or reads via Web access. If, or when, I'm found out, I can always insist that this is totally for national security, to help catch terrorists, and that citizens with nothing to hide have no reason to worry. Isn't that what the East Germans and the Nazis said? [Note that savvy tech users who monitor their outgoing connections should be able to spot something odd going on, and even block it. That situation could require more collaboration with Symantec, McAfee – require them to allow the NSA to access users' systems from Symantec, and McAfee IP addresses.]

What if there's too much pushback on plan B? I can try plan C: Go directly to the major chip companies. That would be Intel, AMD, the ARM companies and any vendor who makes CPU chips for mobile devices. Force them into Prism if they're US companies. If they're not, then put pressure on US mobile phone vendors and carriers to only use CPUs from Prism companies. If I can insert the microcode I want directly into these CPUs, then I own the devices that use them. Doesn't matter what operating system or encryption strategy is used: I get access to whatever files and plain text I want. And it's all for free: I don't even have to pay for network access.

And if plan C doesn't work? Remember that I'm Dr Evil. I have an almost unlimited budget and can operate in near complete secrecy - as long as no more Ed Snowdens show up. So I can always think of more nefarious ways to defeat encryption by finding the money, staff and friendly FISA Court judges to help me succeed. Remember: My goal is to be able to intercept and examine the communications of any network user anywhere on earth. That means you, your family, doctors, lawyers, judges, Congress people, senior executives, Presidents. Don't even think about reducing my budget or imposing oversight because I know all your secrets and can easily blackmail you.

Ok, let's turn off Dr Evil. As far as I know, the anti-malware and CPU companies are not in the Prism program. But it could happen.... unless we show a lot more resistance than we have been.

[MK adds: Bruce Schneier addressed the issue of cooperation between companies and the NSA in a series of postings in the August 15, 2013 *Crypto-Gram* < <a href="https://www.schneier.com/crypto-gram-1308.html#1">https://www.schneier.com/crypto-gram-1308.html#1</a> >]

Ric Steinberger < <a href="http://about.me/ricsteinberger">http://about.me/ricsteinberger</a> > is President of Mobile App Research Group < <a href="https://angel.co/mobile-app-research-group">https://angel.co/mobile-app-research-group</a> > and has been teaching in the Norwich University Master of Science in Information Security & Assurance program < <a href="http://infoassurance.norwich.edu/">http://infoassurance.norwich.edu/</a> > since 2006.

\* \* \*

M. E. Kabay,< <a href="mailto:mekabay@gmail.com">mailto:mekabay@gmail.com</a> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.<a href="mailto:http://www.mekabay.com/">http://www.mekabay.com/</a> >

Copyright © 2013 Ric Steinberger. All rights reserved.