## News from the Front: The Changing Face of INFOSEC

## Network World May-June 2001

M. E. Kabay, PhD, CISSP <a href="mailto:rmkabay@compuserve.com">rmkabay@compuserve.com</a>

Copyright © 2001 M. E. Kabay. All rights reserved.



Copyright © 2001 M. E. Kabay. All rights reserved.

## Network World: Changing Security Paradigms

May-June 2001

M. E. Kabay, PhD, CISSP

was at the time this talk was presented Security Leader, INFOSEC Group

AtomicTangerine, Inc.
Menlo Park, CA
http://www.atomictangerine.com

and is currently

Associate Professor of Computer Information Systems Norwich University, Northfield, VT

He can be reached by mail at 255 Flood Road Barre, VT 05641-4060

Telephone and voice mail: 802-479-7937

## **Objectives**

- Review fundamental goals of INFOSEC
- Raise awareness of key challenges
- Examine defensive strategies
- Review practical recommendations
- Set common ground for vendor presentations



opyright © 2001 M. E. Kabay. All rights reserved.

#### About Michel E. Kabay

M. E. Kabay began learning assembler at age 15 and had learned FORTRAN IV G at McGill University by 1966. In 1976, he received his PhD from Dartmouth College in applied statistics and invertebrate zoology. Until 1979, he was a university professor in applied statistics. In 1979, he joined a compiler team for a new 4GL and RDBMS in the U.S., being responsible for developing the statistical syntax, writing the parser, error traps and code generation for statistical functions in the command language. Kabay joined Hewlett\_Packard in 1980 and became a performance specialist, winning the Systems Engineer of the Year Award in 1982. After a few years working in a large service bureau as operations manager, he formed his own company in 1986. Kabay has specialized in consulting and training for systems performance, systems operations, and systems security. He has written security columns for Computer World, Network World, Computing Canada, Secure Computing Magazine, NCSA News, Information Security Magazine and several other trade magazines. He attained the status of Certified Systems Security Professional (CISSP) in 1997.

Dr Kabay has published over 350 technical papers in operations management and security and completed a college textbook, *The NCSA Guide to Enterprise Security: Protecting Information Assets* (ISBN 0-07-033147-2) published by McGraw-Hill in April 1996. He won the Best Paper Award at the 16th National Computer Security Conference in 1993 for his submission, Social Psychology and INFOSEC: Psychosocial Factors in the Implementation of Information Security Policy. Kabay was the leader of the International Delegation of Computer Security Experts to China in April 1994 organized by the Citizen Ambassador Program. He was the Program Chair for the First and Second International Conferences on Information Warfare in Montreal in 1993 and 1995 and has lectured at the US Army War College, the NATO Lathe Gambit counter-intelligence project and NATO HQ in Brussels. Kabay was Security Leader of the INFOSEC Group of AtomicTangerine from January 2000 through June 2001 and is now Associate Professor of Computer Information Systems at Norwich University, Northfield, VT. He is currently working feverishly as the Technical Editor of the Computer Security Handbook, Fourth Edition to be published by Wiley in April 2002.

### **Overview**

- Fundamental Elements of INFOSEC
- Major challenges for information security today
- Strategic responses
- Grounds for hope
- Recommendations



opyright © 2001 M. E. Kabay. All rights reserved.

#### Books and Other Resources for Beginners in INFOSEC.

Campen, A. D., D. H. Dearth, & R. T. Goodden, eds. (1996). *Cyberwar: Security, Strategy, and Conflict in the Information Age*. AFCEA International Press (Fairfax, VA). ISBN 0-916159-26-4. vii + 296.

Fialka, J. J. (1997). *War by Other Means: Economic Espionage in America*. W. W. Norton (New York). ISBN 0-393-04014-3. xiv + 242. Index.

Forester, T. & P. Morrison (1990). *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing*. MIT Press (Cambridge, MA). ISBN 0-262-06131-7. vi + 193. Index.

Freedman, D. H. & C. C. Mann (1997). *@Large: The strange case of the world's biggest Internet invasion.* Simon & Schuster (New York). ISBN 0-684-82464-7. 315 pp. Index.

Garfinkel, S. (2000). *Database Nation: The Death of Privacy in the 21st Century*. O'Reilly (Sebastopol, CA). ISBN 1-56592-653-6. vii + 312. Index.

Goodell, J. (1996). *The Cyberthief and the Samurai: The True Story of Kevin Mitnick--and the Man Who Hunted Him Down.* Dell (New York). ISBN 0-440-22205-2. xix + 328.

Gordon, S. (1993). Inside the mind of Dark Avenger (abridged). Originally published in *Virus News International* (January 1993).

http://www.research.ibm.com/antivirus/SciPapers/Gordon/Avenger.html

Gordon, S. (1994). Technologically enabled crime: Shifting paradigms for the year 2000. Originally published in *Computers and Security*.

http://www.research.ibm.com/antivirus/SciPapers/Gordon/Crime.html

(Cont'd on next page)

### News from the Front

#### Introductory Readings, cont'd

Gordon, S. (2000). Virus writers: The end of innocence? Presented at the 10th International Virus Bulletin Conference. http://www.research.ibm.com/antivirus/SciPapers/VB2000SG.htm and http://www.research.ibm.com/antivirus/SciPapers/VB2000SG.pdf

Hafner, K. & J. Markoff (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. Touchstone Books, Simon & Schuster (New York). ISBN 0-671-77879-X. 368. Index.

Kabay, M. E. (2000). Making ethical decisions: A guide for kids (and parents and teachers too). http://www.securityportal.com/kfiles/files/ethicaldecisions.html

Littman, J. (1996). *The Fugitive Game: Online with Kevin Mitnick--The Inside Story of the Great Cyberchase.* Little, Brown and Company (Boston). ISBN 0-316-5258-7. x + 383.

Power, R. (2000). *Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace*. Que. ISBN: 0-78972-443-X. 450 pp.

Schwartau, W. (1991). *Terminal Compromise* (novel). Inter.Pact Press (Seminole, FL). ISBN 0-962-87000-5. 562 pp.

Shimomura, T. & J. Markoff (1996). *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw--by the Man Who Did It.* Hyperion (New York). ISBN 0-7868-6210-6. xii + 324. Index.

Slatalla, M. & J. Quittner (1995). *Masters of Deception: The Gang that Ruled Cyberspace*. HarperCollins (New York). ISBN 0-06-017030-1. 225 pp.

Smith, G. (1994). *The Virus Creation Labs: A Journey into the Underground*. American Eagle Publications (Tucson, AZ). ISBN 0-929408-09-8. 172 pp.

Sterling, B. (1992). *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. Bantam Doubleday Dell (New York). ISBN 0-553-08058-X. xiv + 328. Index.

Stoll, C. (1989). The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. Pocket Books (Simon & Schuster, New York). ISBN 0-671-72688-9. viii + 356.

Winkler, I. (1997). *Corporate Espionage: What it is, why it is happening in your company, what you must do about it.* Prima Publishing (Rocklin, CA). ISBN 0-7615-0840-6.

## Fundamental Elements of INFOSEC:

#### Overview:

Protect the 6 atomic elements of INFOSEC:

- Confidentiality
- Possession or control
- Integrity
- Authenticity
- Availability
- Utility



Copyright © 2001 M. E. Kabay. All rights reserved.

These six elements are sometimes called the *Parkerian Hexad* in contrast with the *Classic Triad* of confidentiality, integrity and availability.

For extensive discussion of these issues, see

- Parker, D. B. (1998) Fighting Computer Crime: A New Framework for Protecting Information. Wiley (NY) ISBN 0-471-16378-3. xv + 500 pp; index
- Kabay, M. E. (1996). *The NCSA Guide to Enterprise Security: Protecting Information Assets.* McGraw-Hill (New York). ISBN 0-07-033147-2. xii + 388 pp. Index.

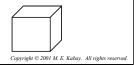
·				

## Confidentiality

### Restricting access to data

- Protecting against unauthorized disclosure of existence of data
  - E.g., allowing industrial spy to deduce nature of clientele by looking at directory names
- Protecting against unauthorized disclosure of details of data
  - E.g., allowing 13-yr old girl to examine HIV+ records in Florida clinic





- The Canadian consumer-tracking service Air Miles inadvertently left 50,000 records of applicants for its loyalty program publicly accessible on their Web site for an undetermined length of time. The Web site was offline as of 21 January until the problem was fixed.
- 2. An error in the configuration or programming of the F. A. O. Schwarz Web site resulted paradoxically in weakening the security of transactions deliberately completed by FAX instead of through SSL. Customers who declined to send their credit-card numbers via SSL ended up having their personal details address and so forth stored in a Web page that could be accessed by anyone entering a URL with an appropriate (even if randomly chosen) numerical component.
- 3. Prof. Ross Anderson of Cambridge University analyzed requirements on the AMAZON.COM online bookstore for credit card number, password, and personal details such as phone number. He identified several risks: (1) merchant retention of credit card numbers poses a far higher risk of capture than of capture in transit; (2) adding a password increases the likelihood of compromise because so many naïve users choose bad passwords and then write them down; (3) even the British site for Amazon contravenes European rules on protecting consumer privacy; (3) such practices make it easier for banks to reject their clients' claims of fraudulent use of their credit-card numbers.

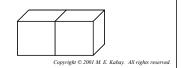
٠			

Possession

**Control over information** 

- Preventing physical contact with data
  - E.g., case of thief who recorded ATM PINs by radio (but never looked at them)
- Preventing copying or unauthorized use of intellectual property
  - E.g., violations by software pirates

NetworkWorld seminars and events



7

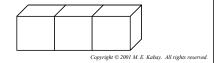
- 1. In Beijing, a court ordered two software pirates to compensate Microsoft for stealing their software and making illegal copies. This was the first case in which the Chinese justice system condemned miscreants for violations of intellectual property rights.
- 2. Hitachi, IBM, NEC, Pioneer and Sony (the ""Galaxy Group"") announced their agreement on a new digital watermark standard that would embed a cryptographic code in every frame of a digital multimedia work. New digital equipment would not allow copies of such works."
- 3. The Norwegian company FAST makes software that can download MP3 files. The International Federation of the Phonographic Industry (IFPI) lodged a complaint that resulted in criminal prosecution of FAST for facilitating the theft of illegally posted copyrighted music from the Web. The IFPI was also contemplating a complaint against Lycos, whose search engine catalogs these illegal snippets of intellectual property.
- 4. The recent fuss over Napster and related peer-to-peer distribution channels for trading pirated music is an example of concern over possession or control of intellectual property.

Integrity

Internal consistency, validity, fitness for use

- Avoiding physical corruption
  - E.g., database pointers trashed or data garbled
- Avoiding logical corruption
  - E.g., inconsistencies between order header total sale & sum of costs of details





8

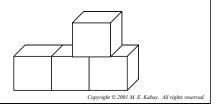
- Sun Valley, ID uses a computer-based identification and authorization system using a computer-generated pass with a bar code, radio-linked scanners and computers, and so on. The system works very well. Unfortunately, after a hard disk crash in mid-December 1997, the operators found that surprise they had no backups for the data they lost. Thousands of users were asked to re-register with the area.
- 2. At the Stanford University Graduate School of Business, system administrators installed additional disk capacity to their servers. They then reloaded files from a corrupt backup tape on 7 Mar. The faculty and student files were destroyed, leaving many faculty members and graduate students without their research files. [This incident again demonstrates the importance of VERIFYING THE READABILITY of backups. It also strengthens my belief in the wisdom of making TWO backups before attempting to reload a system.]
- 3. The RAND Corporation reported that CD-ROMs can deteriorate within 5-10 years -- much faster than the 50 years usually quoted. This instability is quite apart from the even more serious problem of incompatibility of medium, where a perfectly good storage device becomes unreadable because of changes in technology. Ever try to read an 8-inch floppy disk from the 1970s on your DVD player?
- 4. Pity Mr Cody Johnston, a commercial trucker in Bozeman, MT. He admittedly broke speeding laws and paid a fine, but the local newspaper reported his misdemeanor as a sexual deviation charge, which potentially includes homosexuality and bestiality. Apparently the court computer system printed out a list of convictions using erroneous labels for the internal codes. Mr Johnston sued the court and the newspaper for libel.
- 5. A Social Security Administration employee who become angry with a woman with whom he argued in an Internet chat room used a fellow-employee's terminal to fill in a death date for the woman in her SSA records. She applied for a loan at her bank and discovered that she was ""cyberdead."" Jorge Yong admitted culpability, resigned and paid \$800 in fines and damages.

## **Authenticity**

### Correspondence to intended meaning

- Avoiding nonsense
  - E.g., part number field actually contains cost
- Avoiding fraud
  - E.g., sender's name on e-mail is changed to someone else's





9

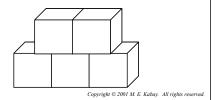
- 1. According to the British National Criminal Intelligence Service, the explosion in credit-card counterfeiting and other credit fraud is largely due to increased activity by Asian Triads. Losses grew by 500% between 1991 and 1998, with total theft estimated at £25M in the UK in 1998.
- 2. In Newmarket, Ontario (near Toronto), thieves in cahoots with a gas-station employee installed a miniature camera focused on the debit-card PIN pad. Videos of customers punching in their PINs, coupled with account information provided by the criminal employee sufficed to let the gang create fake debit cards to pillage accounts. The criminals got into the habit of visiting ATMs at midnight so they could steal two days' worth of maximum withdrawals. Police reported total thefts in the hundreds of thousands of dollars. The criminals were arrested just before a planned expansion to five more gas stations.
- 3. The Transportation Federal Credit Union was robbed of over \$1M by Asian crime groups which developed algorithms for generating valid debit-card numbers (with a success rate of about 50%). The fake cards were then used to extract money from the victimized accounts. Unfortunately, a software error at the Union precluded verification of the encrypted checksums on the cards' magnetic strips.
- 4. In Finland, high-tech thieves installed a ""small black card reader"" on top of the regular slot for inserting debit and credit cards in an ATM. With the codes from their extra card reader plus some standard shoulder-surfing to garner PINs, the thieves were able to create 60 counterfeit cards and stole the equivalent of U\$36,600.
- 5. A father and his teenaged daughter were arrested in Michigan after allegedly using a scanner, computer, and color printer to create counterfeit U\$20 bills and spending \$2,800 of the fake money on Christmas presents. Donald Gill of Fairgrove, MI was held in jail pending Federal felony charges. His 17-year-old girl was released on bail and charged under state laws (minors are not subject to federal felony laws).

## **Availability**

### Timely access to data

- Avoid delays
  - E.g., prevent system crashes & arrange for recovery plans
- Avoid inconvenience
  - E.g., prevent mislabeling of files





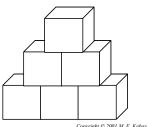
- 1. Installation of some new software on the ETrade Web-based stock brokerage caused intermittent, serious failures that interrupted electronic trading for several hours on Wednesday 3 February 1999. Some customers interviewed by R. Scott Raynovich, writing for Wired, stated that they would pull their brokerage business out of Etrade for failing to provide consistent service. An anonymous investor reportedly said, "I'm trusting these guys with thousands of dollars of my money, and they can't provide me consistent access to it," said one ETrade customer, who asked to remain unnamed because he feared retribution from ETrade officials as he attempted to transfer money to another service. Hours, sometimes days, go by with me unable to put money into a suddenly hot stock, pull out of one that's tanking, or try to get in on an IPO. I'm disgusted with this company."
- 2. The Charles Schwab online stock brokerage computers went down at 09:37 on 1999-02-24 for about 90 minutes, causing disruption for its clients, who were normally placing an average of 153,000 trades a day online 28% of the market for online securities trading.
- 3. On 21 Feb 1999, there was a 15 hour period when many ISPs in the UK were down due to (1) a problem on a transatlantic link maintained by Teleglobe and (2) the simultaneous upgrade of a mail server on the Cable Internet ISP. Malcolm Park noted in RISKS that many users of the affected ISPs complained about interference with their Net-dependent business. He pointed out that businesses should know that the Internet has no guarantee of service; at the very least, it would be appropriate for anyone dependent on the Net to have a contract with a backup ISP. [MK comments: here in Vermont, I have two ISPs -- and have often had to resort to the secondary one when the first one's local node is saturated or malfunctioning. Unfortunately, I still have only one set of wires between our home out in the boondocks and the central switch -- but at least the set includes three different phone numbers.]
- 4. In February 2000, distributed denial-of-service attacks seriously impeded traffic on prominent Web sites such as Amazon.com and eBay.com. Criminals installed unauthorized *zombie* software onto thousands of unprotected Web servers and then coordinated their bursts of unwanted traffic using encrypted messages sent from *master* programs. The volume of the spurious traffic overwhelmed some servers, causing crashes, and blocked thousands of users from reaching the targeted Web sites due to bandwidth saturation.

## Utility

### Usefulness for specific purposes

- Avoid conversion to less useful form
  - E.g., replacing dollar amounts by foreign currency equivalent
- Prevent impenetrable coding
  - E.g., employee encrypts source code and "forgets" decryption key





- 1. The entire Y2K debacle was a case of a change in the environment's rendering a data storage format less *useful* than it was previously.
- 2. In my own practice, I was called in to improve performance for a large data center in 1989 where the batch processing was overlapping with the start of the day shift. The system was running a scheduling program, so I naturally asked to see the source code. Red-faced, the sysadmins admitted that they had no source code. Seemed the vendor who wrote the system claimed they had turned over the magnetic tapes back in 1983 when they completed the software, but no one in the center had any record of the delivery or knew where the tapes might be. The absence of the source code made the system less useful because all changes had to be done by patching the executable code a complex and risk business even with source code available, but a real gamble without the source.

<u> </u>		

### **Overview**

- Fundamental Elements of INFOSEC
- Major challenges for information security today
- Strategic responses
- Grounds for hope
- Recommendations



opyright © 2001 M. E. Kabay. All rights reserved.

### **Gene Spafford Challenges Complacency**

by M. E. Kabay, PhD, CISSP/ Security Leader, INFOSEC Group, Atomic Tangerine, Inc.

I would like to draw readers' attention to the remarks made by Prof. Eugene Spafford of Purdue University on the occasion of his receiving the National Computer Systems Security Award from the National Computer Security Center at the 23rd (and last) National Information Systems Security Conference in Baltimore, 16 October 2000.

On his biographical page at < http://www.cerias.purdue.edu/homes/spaf/ >, we read, "Gene Spafford is a Professor of Computer Sciences at Purdue University, where he has been on the faculty since 1987. His current research interests are primarily in the areas of information security, computer crime investigation and information ethics. He also has an appointment as a Professor of Philosophy at Purdue.

"Spaf (as he is known to his friends, colleagues, and students) is director of the Purdue CERIAS (Center for Education and Research in Information Assurance and Security), and was the founder and director of the (now superseded) COAST Laboratory. He is also the interim Information Systems Security Officer for Purdue University. Related to this, he is the founder and de facto director of the PCERT (Purdue Computer Emergency Response Team)."

In his plenary address to the Conference, Spaf made the following key points about the state of information security today (I am summarizing and paraphrasing Spaf's words):

- Security is going to get worse before it gets better because of human nature, including the
  people who design, write, deploy, use and abuse the systems and even because of the
  people who guard the systems.
- Some software manufacturers have perceived security problems such as viruses to be someone else's problem. (Cont'd on next page)

### News from the Front

- Scanning for viruses using known search strings doesn't work for everyone now because many people fail to keep their signature files up to date, but if we reach the projected 100,000 known viruses by 2004, there will be a new virus reported roughly every hour or two and how will downloading signatures keep up with that threat?
- We are at risk in part because we have entrusted security to users who lack understanding and training in how to cope with the issues.
- Programmers and system administrators are inadequately trained, with enormous time
  wasted due to program and system crashes. In addition, known vulnerabilities remain
  unpatched on uncounted systems.
- Senior executives select software and hardware based on initial cost of acquisition instead of long-term operational costs and risk analysis. New features are assigned higher value than reliability.
- The software industry, aware of the problems its members are causing, includes supporters of the UCITA [the Uniform Computer Information Transactions Act] which would help "shield themselves from consequences of shoddy practices, and even to prevent critical public comment on their wares. (I [Spaf] would strongly urge you to educate yourselves about the awful consequences if UCITA is passed in your states; see my [Spaf's] editorial in issue E38 of the IEEE Cipher as a starting point or refer to < http://www.4cite.org >.)"

Spaf issued the following challenges to everyone involved with information technology:

- Commit to thinking about the foundations of security in software instead of patching fundamentally flawed systems.
- Hold companies liable for bad products that fail because of faulty design and operation.
- Stop ridiculing "stupid user tricks" and design systems to take into account the nature of people for whom computers are equivalent to appliances.
- Improve the education of computer programmers and others who will be involved in creating and managing systems. Include human factors in students' education so they can address real-world problems. Apply interdisciplinary perspectives.

\* \* \*

Please see the page of information about the event at

< http://www.cerias.purdue.edu/homes/spaf/ncssa.html > and read the full text of Spaf's remarks. Each one of his points is worthy of extended thought and discussion.

This article was published in the Network World Fusion Security Newsletter. For archives of published columns, see

< http://www.nwfusion.com/newsletters/sec >.

## Major Challenges for Information Security Today

#### Overview:

- Users don't take security seriously
- Management does not take security seriously
- Changing technical environment
- Current and emerging security incorrectly viewed as adequate
- Legal issues



Copyright © 2001 M. E. Kabay. All rights reserved.

For an analysis of some of these issues, see the following series of articles published in the Network World Fusion newsletter:

Kabay, M.E. (2000)

- Los Alamos Redux. (2000-07-10) http://www.nwfusion.com/newsletters/sec/2000/0710sec1.html
- Los Alamos Redux, Part 2. (2000-07-12) http://www.nwfusion.com/newsletters/sec/2000/0710sec2.html
- Los Alamos Redux, Part 3. (2000-07-17) http://www.nwfusion.com/newsletters/sec/2000/0717sec1.html

## Users Don't Take Security Seriously

#### Overview:

- Novice computer users
- Generation gap
- Under-trained staff



opyright © 2001 M. E. Kabay. All rights reserved.

The following section looks at elements of the enterprise culture. For a review of how social psychology plays a role in developing and implementing security policies, see Kabay, M. E. (2000)

- What's important for information security: A manager's guide. http://www.securityportal.com/kfiles/files/infosecimportant.html
- Securing your business in the age of the Internet. http://www.securityportal.com/kfiles/files/securingbusiness.html

## **Novice Computer Users**

- Explosive growth of Net, WWW
- Hundreds of millions of users
- Gullible victims of
  - viruses, Trojans, joke programs
  - "spam," chain mail, hoaxes
  - fraud

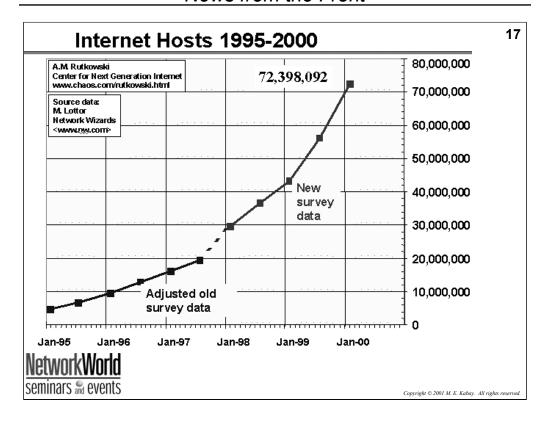


Copyright © 2001 M. E. Kabay. All rights reserved.

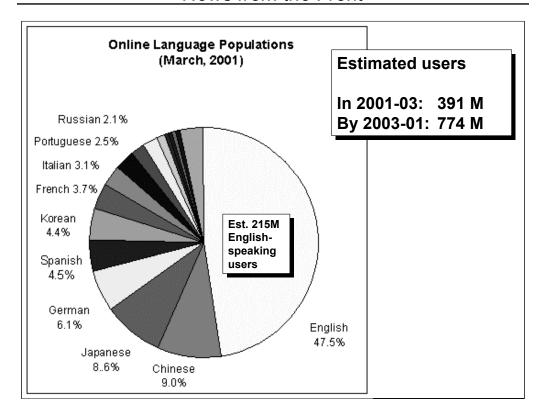
How big is the Internet? The answers depend on what aspect you are considering.

- For a picture of the interconnectivity on the Internet, see *Internet: The Big Picture* by Russ Haynal at
  - http://navigators.com/internet architecture.html
- Haynal also has a list of links to statistics about the growth of the 'Net: <a href="http://navigators.com/stats.html">http://navigators.com/stats.html</a>

•	
•	
•	
	 -



http://navigators.com/statall.gif			



#### http://www.euromktg.com/globstats/

See also "How Many Online" from the NUA Internet Surveys site at

< http://www.nua.ie/surveys/how\_many\_online/index.html > which suggest the following guesses:

World Total 407.1 million
Africa 3.11 million
Asia/Pacific 104.88 million
Europe 113.14 million
Middle East 2.40 million
Canada & USA 167.12 million
Latin America 16.45 million

## Generation Gap

- Parents and teachers know less than kids
- Adults violate intellectual property laws
- Press glorify criminal hackers
- Children victims of pornographers and pedophiles



opyright © 2001 M. E. Kabay. All rights reserved.

Grunwald Associates: Soaring Net Use by Children & Teenagers

- Jun 09 2000: The number of 2-17 year olds online in the US has tripled to 25 million since 1997, when 8 million children and teenagers had Internet access, according to a new study from Grunwald Associates.
- The study says that this growth in the number of children online has been fuelled by the boom in the number of mothers logging onto the Internet. There were 4.5 million moms online in 1997 and this rose to 16.4 million by the end of last year.
- Parents are motivated to buy PCs and get Internet access because they believe their children will benefit educationally from using the Internet.
- About 46 percent of all family homes now have Internet access, but by 2005, more children will go online at school than at home

From: <a href="http://www.nua.ie/surveys/?f=VS&art\_id=905355832&rel=true">http://www.nua.ie/surveys/?f=VS&art\_id=905355832&rel=true</a>

Gartner Group: Cybercriminals could hoodwink masses

- Apr 05 2001: Gartner has warned that cybercriminals could defraud millions of online consumes in an act of "economic mass victimization" some time in the next two years.
- Online fraudsters could steal small amounts of money in the same way from large numbers of consumers. . . .
- Gartner believes that the economic cost of cybercrime could escalate by anywhere between 1000 and 10,000 percent by the end of 2004.
- The company advises consumers to protect themselves by erecting firewalls and checking credit card statements carefully.

From: <a href="http://www.nua.ie/surveys/?f=VS&art\_id=905356635&rel=true">http://www.nua.ie/surveys/?f=VS&art\_id=905356635&rel=true</a>

## **Under-Trained Staff**

- Minimal training
- Secretaries and office managers responsible for Web sites, LANs
- Years-old vulnerabilities left in place
- Under-protected systems are hosts for zombies in DDoS



Copyright © 2001 M. E. Kabay. All rights reserved.

1.	When the Defense Information Systems Agency (DISA) tested 38,000 unclassified networked Defense Department computers between 1994 and 1997, the penetration testers were able to gain unauthorized access to 66% of the systems because of known, documented vulnerabilities even though there were well-documented, easily-available free patches to prevent the exploits. Many of the vulnerabilities had solutions that were many years old.

## Major Challenges for Information Security Today

#### Overview:

- Users don't take security seriously
- Management does not take security seriously
- Changing technical environment
- Current and emerging security incorrectly viewed as adequate
- Legal issues



Copyright © 2001 M. E. Kabay. All rights reserved.

InfoWorld: CIOs trust their network security

- Jan 08 2001: Although cybercrime is on the increase, the vast majority of chief information officers (CIOs) have confidence in their companies' network security, according to a recent survey.
- More than 90 percent of the 1,400 CIOs polled in RHI Consulting's survey believe their networks are safe from internal and external security breaches.
- RHI said that the high level of confidence could be partly due to increased spending on hardware, software, and network-security personnel in recent times. In a separate RHI survey in August, 58 percent of CIOs said they had increased their investment in corporate network security initiatives.
- With a slowdown expected in corporate IT spending, it remains to be seen whether CIOs can maintain this level of confidence throughout 2001. As reported by the Financial Times, a survey of CIOs released last week found that growth in US corporate IT budgets will be a lot slower this year, at just 5 percent, than the 11 percent growth rate experienced in 2000.
- After considerable investment in Y2K solutions over the last two years, IT services spending will be cut back in 2001, while the biggest growth (19 percent) will be in software spending.
- Corporate spending on IT in Europe looks set to continue growing strongly, with a rise of 13 percent expected this year, down just 1 percent on last year's figures.

From: http://www.nua.ie/surveys/?f=VS&art id=905356318&rel=true

## Management Does Not Take Security Seriously

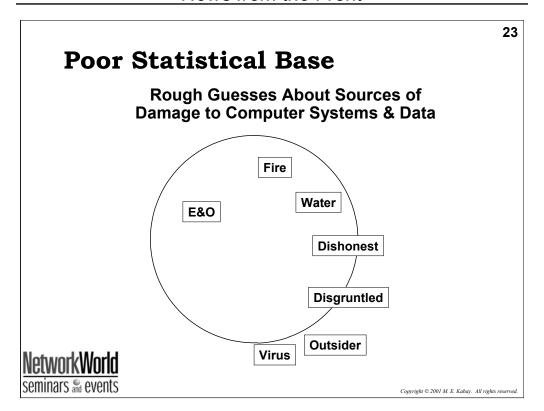
#### Overview:

- Poor statistical base for risk management
- Difficult to make business case for strong security
- Security inconsistent with main line of business
- Strong security may run counter to organizational culture
- Corporate management resists user restrictions
- Short-term management horizon



Copyright © 2001 M. E. Kabay. All rights reserved

See					
Kabay, M. E. (2000). A rant about InfoSec.					
http://www.securityportal.com/kfiles/files/infosecrant.html					



Limitations on Our Knowledge of Computer Crime

There are two fundamental difficulties preventing us from developing accurate statistics of this kind. These difficulties are known as the problems of ascertainment.

#### **Detection**

The first problem is that an unknown number of crimes of all kinds are undetected. For example, even outside the computer crime field, we don't know how many financial frauds are being perpetrated. We don't know because some of them are not detected. How do we know they're not detected? Because some frauds are discovered long after they have occurred. Similarly, computer crimes may not be detected by their victims but may be reported by the perpetrators.

A commonly-held view within the information security community is that only one-tenth or so of all the crimes committed against and using computer systems are detected.

#### Reporting

The second problem of ascertainment is that even if attacks are detected, it seems that few are reported in a way that allows systematic data collection. This belief is based in part on the unquantified experience of information security professionals who have conducted interviews of their clients; it turns out that only about ten percent of the attacks against computer systems revealed in such interviews were ever reported to any kind of authority or to the public.

Given these problems of ascertainment, computer crime statistics should generally be treated with skepticism.

## Poor Statistical Base for Risk Management

- No mandatory reporting
- Difficult to convince CFOs of importance
- Lack sound probabilities for calculating expected loss
- Little insurance available
  - Expensive



ppyright © 2001 M. E. Kabay. All rights reserved.

1. The FBI's InfraGard project may encourage participants to improve the statistical database. From the official Web site ( <a href="http://www.infragard.net/">http://www.infragard.net/</a>):

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a cooperative undertaking between the U.S. Government (led by the FBI and the NIPC) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures.

All InfraGard participants are committed to the proposition that a robust exchange of information about threats to and actual attacks on these critical infrastructures is an important element for successful infrastructure protection efforts.

The goal of InfraGard is to enable that information flow so that the owners and operators of infrastructure assets can better protect themselves and so that the United States government can better discharge its law enforcement and national security responsibilities.

(Continued on next page)


### News from the Front

2. The Information Sharing and Analysis Centers (ISACs) are sector-specific groupings for more specialized and technical information sharing.

The following text is from the *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 May 22, 1998* at <a href="http://www.nipc.gov/about/pdd63.htm">http://www.nipc.gov/about/pdd63.htm</a>

Information Sharing and Analysis Center (ISAC): The National Coordinator [the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism will be appointed by and report to the President through the Assistant to the President for National Security Affairs], working with Sector Coordinators, Sector Liaison Officials and the National Economic Council, shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center. The actual design and functions of the center and its relation to the NIPC [National Infrastructure Protection Center] will be determined by the private sector, in consultation with and with assistance from the Federal Government. Within 180 days of this directive, the National Coordinator, with the assistance of the CICG [Critical Infrastructure Coordination Group] including the National Economic Council, shall identify possible methods of providing federal assistance to facilitate the startup of an ISAC.

Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC. The center could also gather, analyze and disseminate information from the NIPC for further distribution to the private sector. While crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the government. As ultimately designed by private sector representatives, the ISAC may emulate particular aspects of such institutions as the Centers for Disease Control and Prevention that have proved highly effective, particularly its extensive interchanges with the private and non-federal sectors.

Under such a model, the ISAC would possess a large degree of technical focus and expertise and non-regulatory and non-law enforcement missions. It would establish baseline statistics and patterns on the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used by the private sector and, as deemed appropriate by the ISAC, by the government. Critical to the success of such an institution would be its timeliness, accessibility, coordination, flexibility, utility and acceptability.

3. For a more detailed examination of computer crime research methods and results, see *Understanding Studies and Surveys of Computer Crime* at

http://securityportal.com/articles/studiesandsurveys20001212.html

This review is intended to provide guidance for critical reading of research results about computer crime. It will also alert designers of research instruments to the need for professional support in developing questionnaires and analyzing results.

Studies and Surveys of Computer Crime at http://www.securityportal.com/kfiles/research.html

This article reviews recent reports about computer crime and computer criminals, principles for critical reading of research results published in the popular and technical press, and highlights of interview and survey studies of computer crimes and computer criminals.

## **Annualized Loss Expectancies (ALE)**





onvright © 2001 M. F. Kahav. All rights reserved

- For discussions of ALE, see Krause and Tipton (1997) at http://secinf.net/info/misc/handbook/229-230.html
  - and also Kabay, M. E. (1996). *The NCSA Guide to Enterprise Security: Protecting Information Assets.* McGraw-Hill (New York). ISBN 0-07-033147-2. xii + 388 pp. Index.
- 2. A simple example of the expected value calculation is any gambling calculation. E.g., if someone wagers \$1 on a single number in a roulette game with 36 winning numbers and two numbers (0 and 00) giving all advantage to the house, then their expected loss is

Probability(win) \* Win + Probability(loss) \* Bet

and the calculation is

$$(1/38) * $36 + (37/38) * (-$1) = -$0.02632.$$

In other words, every bet of a dollar on a roulette wheel has an average likelihood of losing more than two cents for the person betting against the house.

3. Similarly, a risk management methodology can be viewed as having an annualized loss expectancy calculated by making a "win" equivalent to having a recovery management plan in place when an event occurs and avoiding the cost of the event. A "loss" would be equivalent to spending money on the recovery management plan but never using it. Thus one could write

Probability(event) \* (money saved) + Probability(no event) \* (money spent).

For example, if the security event were to cost \$10,000,000 and have an annualized probability of 0.001 but the cost of avoiding the damage were \$1,000, then the annualized loss expectancy for this strategy would be calculated as

$$0.001 * $10,000,000 + 0.999 * (- $1,000) = $10,000 - $999 = $9,001$$

In other words, this hypothetical strategy would be expected, on average, to save \$9,001 per year by avoiding losses.

## Difficult to Make Business Case for Strong Security

- Lack of accurate data on intrusions and accidents
  - Difficult to use quantitative risk management
  - But majority of incidents are insider crime
- "Little-old-worthless-me" syndrome
  - Nothing of value to steal
  - No reason to be targeted
  - But systems are compromised daily
    - As springboards for attacks on others
    - · For political purposes
    - · For childish fun
- Security through obscurity is no security at all



Copyright © 2001 M. E. Kabay. All rights reserved.

#### IDC Research: Security breaches provide wake-up call

Feb 16 2001: A new report from IDC has found that the key impetus for companies adopting security technology, is when they suffer a security breach in their organization.

The North American study also found that increased Internet use, the implementation of virtual private networks, and ebusiness projects also drive companies to adopt new security technology.

IDC points out that for companies involved in ebusiness, security and privacy options are core elements for conducting business. Of the 1,000 companies who responded to the survey, practically all were adopting or using security, but the ability to effectively respond to a security breach varied widely by industry.

Anti-virus software is the most common security technology, while hardware-based firewall systems and intrusion-detection solutions are also popular. The banking, financial services, healthcare services, communications, utilities, and government industries are the most proactive in adopting security. In contrast security is rarely considered in the retail industry.

The most common form of security problem is a virus infection at client or server level, with 90 percent of respondents saying their organization had been hit by a virus. Companies involved in retail, education, engineering, management, healthcare services, and transportation had the most difficulty in identifying and eliminating viruses.

From: <a href="http://www.nua.ie/surveys/?f=VS&art\_id=905356465&rel=true">http://www.nua.ie/surveys/?f=VS&art\_id=905356465&rel=true</a>

(the gap in the URL above is an underscore character, "\_").

## **Security Inconsistent With Main Line of Business**

- Information systems viewed as mere infrastructure
- Systems often neglected
  - No upgrades
  - Little maintenance
  - "Not our business"
- Lack of awareness of critical dependence on system confidentiality, availability, integrity, authenticity, control, utility
- But security is no longer just loss avoidance



Copyright © 2001 M. E. Kabay. All rights reserved.

- Information systems can be significant contributors to *strategic* measures such as
  providing *competitive advantage* against more conventional providers of services. E.g.,
  manufacturer can use Web interface, real-time inventory systems and just-in-time delivery
  agreements to provide full customization to a customer instead of only selection from
  limited varieties or models.
- 2. In today's world of e-commerce, many customers decide whether to do business with an organization by how confident they feel about the security of their personal data and transactions.
- 3. See Worstell, K., M. Gerdes & M. E. Kabay (2000). Net present value of information security. <a href="http://securityportal.com/cover/coverstory20001023.html">http://securityportal.com/cover/coverstory20001023.html</a>

-	

## Strong Security May Run Counter to Organizational Culture

- Hostile staff
  - "Paranoia"
  - Security viewed as attempt to seize more control by security staff, bureaucrats
- Physical security viewed as strange, intrusive
- Confusing security with power
  - Upper managers seen to ignore security rules
  - Therefore ignoring security a sign of high status
- Changes in connectivity not understood
- Distributed computing resists centralized control



Copyright © 2001 M. E. Kabay. All rights reserved.

#### For example:

- Automatic logoff settings and secure screensavers can interrupt the user's train of thought and generate resentment.
- Restrictions on access to specific types of information slows down innovative actions because employees have to get permission for what would otherwise be a spontaneous exploration of ideas.
- Academic environments are particularly hostile to security measures.
- Before computers and networks were widely used, a few upper executives used to carry
  huge bunches of master keys around; the same personality types now demand complete
  access to all systems simply because it makes them feel powerful.
- 5. Setting up one's own department LAN or Web site without consulting corporate IT or respecting corporate policies (if any exist) is sometimes viewed as demonstrating a cando, take-charge spirit of innovation, which it may indeed be. However, such independent measures can also result in catastrophic security breaches, inordinate expenses for individual copies of software for which existing corporate licenses exist, increased technical support difficulties, and unpredictable effects on overall network security and performance.

_			
_			
_			
_			

## **Corporate Management Resists User Restrictions**

- Security viewed as restricting rights and freedoms of employees
- Increased technical security viewed as degrading system performance
- Some people associate access with status
- Staff sometimes lack facts and opportunities to counter myths and misperceptions from upper management



Copyright © 2001 M. E. Kabay. All rights reserved.

#### For example:

- Security measures slow down access to systems by *authorized* users (e.g,. Use of tokens, biometrics, passwords).
- Imposing security after an organization has been security-free is usually traumatic.
- Virtual private networks using *inadequate* hardware or software solutions can significantly degrade network throughput.
- Firewalls and content filters *can* interfere with legitimate attempts to carry out research.
- Security and network management personnel are usually so overworked that they have little or no time for research to make a strong case in favor of security measures.
- Improperly developed and poorly implemented security measures can generate a climate of hostility and resistance.

## **Short-term Management Horizon**

- Managers rated on quarterly bottom line
- Managers and employees job-hop
- Therefore no advantage to paying money for security or quality assurance when
  - Both cost money
  - Consequences of bad software and bad security can be evaded by moving to another job



Copyright © 2001 M. E. Kabay. All rights reserved.

- 1. According to Liz Warren, writing in *Computer Weekly* ("Remote control: locking in your teleworkers," 2000-06-01, p. 32), ". . . the typical length of employment is 12 to 18 months."
- 2. Davud Foote reports that, "the average length of employment at Internet companies is only eight months" ("Some preventive medicine for cases of dot-com-itis," *Computerworld* 2000-03-20, p. 34).
- 3. For a general perspective on a contrary view that emphasizes the value of other metrics beyond the quarterly bottom line on a profit and loss statement, see "The 7 Laws of Business Success" by Thomas Wood-Young at < <a href="http://www.salestrainingplus.com/salesmark/articles/laws.htm">http://www.salestrainingplus.com/salesmark/articles/laws.htm</a> >.

## Major Challenges for Information Security Today

#### Overview:

- Users don't take security seriously
- Management does not take security seriously
- Changing technical environment
- Current and emerging security incorrectly viewed as adequate
- Legal issues



opyright © 2001 M. E. Kabay. All rights reserved.

For all of you who do not remember a time before PCs running at 100 MHz or faster:

- 1. When I started programming in 1965, the state-of-the-art data center used an IBM 1401 computer with punch-cards, a single user at a time, and 16 Kb of RAM.
- 2. In 1980, when I was working as as a "systems engineer" for Hewlett-Packard, the biggest computer HP made at the time, the HP3000 Series III the size of a refrigerator got a hardware upgrade that permitted us to double its RAM to 2 Mb. The extra 1 Mb of RAM cost U\$64,000 in 1980 dollars.
- 3. The biggest disk drive HP sold in 1980 was the HP7925; it was the size of a washing machine. It weighed 1500 pounds, needed 240V 3-phase power and air-conditioning. It stored 120 Mb of data and cost U\$25,000 in 1980 dollars.
- 4. A fast modem in 1979 was about 2 feet long by 1 foot high and 1 foot wide; it cost \$1,000 and required 120V AC power. It ran at 300 bps.
- 5. My first useful portable computer was the HP110, which arrived in 1982. It had an LCD screen that showed 80 characters across and 24 lines down, included 2 Mb of RAM that doubled as a RAMDISK, no hard disk, and stored software in ROM; it weighed 7 pounds. The processor ran at 4 MHz. It cost \$4,000. The external hard disk was half a cubic foot in size, weighed 15 pounds, cost \$2,000 and stored 5 Mb.
- 6. HP's first laser printer, the HP2650, was 5 feet high, 4 feet wide and 7 feet long. It cost \$125,000 in 1982 dollars. The maintenance contract for this machine cost \$20,000 a year not counting supplies.
- 7. The fastest hard-wired connection for HP terminals to HP3000 computers in 1984 was 19.2 Kbaud. There was serious doubt at that time that modems would ever go faster than 9600 baud.
- 8. In 1988 I was delighted to buy an ATARI processor running at 16 MHz, with 4 Mb RAM and a laser printer that weighed 40 pounds, was the size of a large grocery box, printed up to 2 pages per minute and cost only \$2,000 in 1988 dollars.

## Changing Technical Environment

- Persistent Internet connections at home
- Peer-to-peer networking
- Proliferating active content
- Automated denial-of-service attacks
- Automated vulnerability scanning
- Cryptography spreading
  - Interfering with law enforcement
  - But massively parallel computing challenges encryption



Copyright © 2001 M. E. Kabay. All rights reserved.

- 1. Persistent Internet connections at home see "Security risks lie beneath broadband hype." (2000-12-13) http://www.nua.ie/surveys/?f=VS&art\_id=905356238&rel=true
- 2. Peer-to-peer networking see "Peer-to-peer software and security." (2000-08-28) http://www.nwfusion.com/newsletters/sec/2000/0828sec1.html
- 3. Proliferating active content see "How ActiveX could be misused." (2001-04-09). <a href="http://www.nwfusion.com/newsletters/sec/2001/00636268.html">http://www.nwfusion.com/newsletters/sec/2001/00636268.html</a>
- 4. Automated denial-of-service attacks see Lessons from Distributed Denial-of-Service Attacks (2000-02-21) <a href="http://www.nwfusion.com/newsletters/sec/0221sec1.html">http://www.nwfusion.com/newsletters/sec/0221sec1.html</a>
- 5. Automated vulnerability scanning see "Unauthorized vulnerability scans." (2000-05-01). <a href="http://www.nwfusion.com/newsletters/sec/0501sec1.html">http://www.nwfusion.com/newsletters/sec/0501sec1.html</a>
- Brute-force cryptanalysis see "Brute Force Attack on UNIX Passwords with SIMD Computer."

	-	

## Major Challenges for Information Security Today

#### Overview:

- Users don't take security seriously
- Management does not take security seriously
- Changing technical environment
- Current and emerging security incorrectly viewed as adequate
- Legal issues



Copyright © 2001 M. E. Kabay. All rights reserved.

vnunet: UK firms know little of technology-related risks

- Mar 14 2001: Despite the publicity surrounding computer viruses and breaches of computer security, most UK companies are ignorant of technology-related risks.
- According to a new study conducted by Mori and sponsored by risk management company Safeonline, there is a "dangerously low level of awareness of risks from technology" among British companies.
- Only 24 percent of large firms and 18 percent of small firms were able to identify risks. Dotcoms fared better, with 63 percent identifying at least one risk posed by their company's use of technology.
- Over half of the businesses polled believed they had adequate protection in place, but the survey found that most of these did not have sufficient security measures. Furthermore, about 60 percent of UK firms do not trust their own IT specialists to protect them adequately.
- Companies do not trust their other employees either. Almost half of those surveyed said their own workers were the most likely source of damage to their computer systems.

From: http://www.nua.ie/surveys/?f=VS&art id=905356556&rel=true

# **Current and Emerging Security Incorrectly Viewed As Adequate**

Overview:

- Most popular operating systems lack security kernel
- Bad quality assurance
- Feature bloat
- Mobile application code uses flawed security model
- IP lacks packet authentication
- Inadequate identification and authentication



Copyright © 2001 M. E. Kabay. All rights reserved.

35

Some general observations about quality and security in technology:

- Executives who have little or no technical background can often make critical decisions on technology. Sometimes it seems as if they choose operating environments using the country-club metric: they've heard someone refer to it positively at their club.
- Making technology decisions on the basis of the attractiveness of its product marketing is equivalent to choosing a mate by how attractively they dress on your first date.
- If the fundamental model of a product is flawed, no amount of patching will keep up with the discovery of exploits.
- Spending more on executive entertainment budgets than on strong identification and authentication is a prescription for overweight executives and lightweight security.
- Beware the top executive who demands a 1.3 GHz Pentium IV processor with 512 Mb of RAM to write memos and get e-mail. This person has confused computing power with personal worth and may extend that confusion to other decisions about information technology.

## Windows 9x Insecurity

- Entire generation of users knows nothing but Windows 9x
- Market penetration 90% in PC arena
- No consideration of security at center of operating system
  - No hierarchy of process privileges
  - All users are root
  - Default status is insecure (e.g., shares)
  - Quality assurance pushed off onto users
- Novice users and managers accept daily (hourly) system failures as normal



Copyright © 2001 M. E. Kabay. All rights reserved.

- Security kernel: (I) "The hardware, firmware, and software elements of a trusted computing base that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct." [NCS04] (See: reference monitor.) (C) That is, a security kernel is an implementation of a reference monitor for a given hardware base." [Shirey, R. (2000). Internet Security Glossary. RFC2828. < <a href="http://www.faqs.org/rfcs/rfc2828.html">http://www.faqs.org/rfcs/rfc2828.html</a>>].
- 2. Kabay, M. E. (2000). "Easter Eggs and the Trusted Computing Base." (2000-03-27) http://www.nwfusion.com/newsletters/sec/0327sec1.html
- 3. Kabay, M. E. (2000). "Monty Python's Flying Circus: Microsoft and the Aircraft Carriers." (2000-08-15)
- 4. Kabay, M. E. (2000). "Feedback from bad operating systems." (2000-04-18) http://www.nwfusion.com/newsletters/sec/0417sec1.html
- 5. After the above (#4) blistering attack on unstable operating systems, I received a message from a puzzled young man in his late teens who wrote, "I don't understand the problem: I reboot my Windows 98 system twice a day and it's fine."

## **Bad Quality Assurance**

- Products released in what would have been called beta-test versions
- Experienced users never install first release
- "Service Packs" are frequently the entire program
- Novices assume that failures are their fault, not program's
- Manufacturers getting away with fraudulent misrepresentation
- Legal moves under UCITA to hamper analysis of flaws
- Shrink-wrap licenses would never be tolerated in other products – user gives away all rights for redress
- New administration almost certain to block productliability lawsuits



- 1. For endless examples of bad quality assurance, see the archives of the RISKS Forum Digest at <a href="http://catless.ncl.ac.uk/Risks/">http://catless.ncl.ac.uk/Risks/</a>
- 2. The "Service Pack 3" for Corel WordPerfect 9.0 is >77MB; the "MS Office 2000 SR-1a update" is >52MB.
- 3. For more information about the UCITA (Uniform Computer Information Transactions Act), see
  - http://www.ucitaonline.com/
  - http://www.ala.org/washoff/ucita/index.html
  - http://www.arl.org/info/frn/copy/ucitapg.html
- 4. Stallman, R. (2000). "Why we must fight UCITA." (2000-02-06). http://linuxtoday.com/stories/15948.html

	-

### **Feature Bloat**

- Document and program no longer distinct entities
- Incorporation of automatic execution of macros
- E-mail programs execute attachments automatically
- Document sizes increasing without limit
- Program size bloated beyond comprehension
- Unpredictable interactions of ponderous programs on bad operating systems = Blue Screen of Death

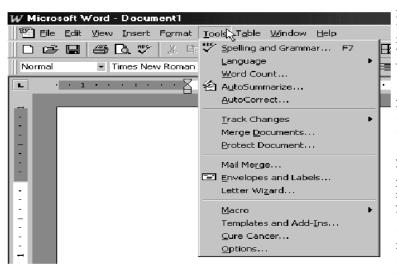


ppyright © 2001 M. E. Kabay. All rights reserved.

http://bbspot.com/News/2000/12/ms\_cancer.html

#### Microsoft Announces Office 10 Will Cure Cancer

Redmond, WA - Microsoft announced yesterday their upcoming version of Office will cure cancer. Many believe this is the killer feature the software giant needs to spur upgrades in its aging Office Suite. Microsoft believes the biggest revenue stream will come from users who purchase the subscription version of Office 10. "When faced with the prospect of their cancer returning at the end of the year, we are pretty confident that they will renew their subscription," said VP of marketing Andy Marskin.



Mr. Marskin denied that the cancer curing feature was included 🖪 because earlier versions of Office actually caused cancer as Linux advocates had suggested. He said, "Those accusations are completely groundless, although we would suggest not pressing CTRL-C too many times unless you really have to."

> "The feature will be fully integrated into each program in the suite," said Microsoft

programmer Halley Grey, "It doesn't matter if a user is developing a presentation in Power Point or working on a spreadsheet in Excel. All they have to do is go the Tools menu and select the <u>Cure Cancer option</u> and it will give them a choice of which cancer they would like cured."

## **Mobile Application Code**

- Java, JavaScript, ActiveX
- Uncertain origins for operational code
- Undocumented "features"
- Laughable security principles: signature is NOT safety (regardless of ActiveX model)



- 1. Felten, E. W. (1997). "Security tradeoffs: Java vs ActiveX. An unofficial view from the Princeton Secure Internet Programming Team." <a href="http://www.cs.princeton.edu/sip/java-vs-activex.html">http://www.cs.princeton.edu/sip/java-vs-activex.html</a>
- 2. "Java Security FAQ." <a href="http://www.cs.princeton.edu/sip/faq/java-faq.php3">http://www.cs.princeton.edu/sip/faq/java-faq.php3</a>
- 3. Kabay, M. E. (2001). "How ActiveX could be misused." (2001-04-09).
- 4. Reavis, J. (1999). "Can Windows play nicely in a sandbox?" (1999-09-15). http://www.nwfusion.com/newsletters/sec/0913sec2.html

### IP Lacks Packet Authentication

- Firewalls usually have no egress filtering configured
  - Forged packets can get into Net easily
- Open SMTP relays give spammers have free reign
  - Forged headers obviate retaliation
- Forged packets allow Denial of Service
  - No way to track real authors



- 1. Moskowitz, R. (2000). "Host identity payload." Internet Draft. (2000-02). <a href="http://www.alternic.org/drafts/drafts-m-n/draft-moskowitz-hip-01.html">http://www.alternic.org/drafts/drafts-m-n/draft-moskowitz-hip-01.html</a>
- 2. MAPS RSS Relay Spam Stopper. http://mail-abuse.org/rss/
- 3. Dave Dittrich's "Distributed Denial of Service (DDoS) Attacks/tools." <a href="http://staff.washington.edu/dittrich/misc/ddos/">http://staff.washington.edu/dittrich/misc/ddos/</a>

_				

## Inadequate I&A

- Still using stupid, ineffective system of passwords
- Managers object to cost of token-based or biometric authentication
  - But costs per employee per year less than a single expense-account meal by executives



- 1. Kabay, M. E. (in press) INFOSEC Year in Review 2000.
  - 2001-01-12: "A 16-year-old boy from the Global Hell gang of criminal hackers was arrested in Eldorado, CA for allegedly stealing user IDs and passwords for 200,000 of the ISP run by Pacific Bell. Police reported that the boy had decrypted 63,000 of the passwords. The lad boasted about his exploits in a chat room; apparently he may have been the hacker responsible for 26 other break-ins, including a computer at Harvard University."
- Kabay, M. E. (1997). INFOSEC Year in Review 1997. http://www.securityportal.com/kfiles/files/iyir1997.pdf
  - 1997-01-02: "A recent survey by Compaq in the financial district of London showed that poor choices are the norm for computer passwords there. A staggering 82% of the respondents said they used, in order of preference, "a sexual position or abusive name for the boss" (30%), their partner's name or nickname (16%), the name of their favorite holiday destination (15%), sports team or player (13%), and whatever they saw first on their desk (8%)."
- O'Shea, T. M. & M. Lee (1999). "Biometric authentication management." http://www.networkcomputing.com/1026/1026f2.html
- Palmgren, K. (2000). "Biometric authentication." (2000-04-24). <a href="http://www.securityportal.com/cover/coverstory20000424.html">http://www.securityportal.com/cover/coverstory20000424.html</a>

# Major Challenges for Information Security Today

#### Overview:

- Users don't take security seriously
- Management does not take security seriously
- Changing technical environment
- Current and emerging security incorrectly viewed as adequate
- Legal issues



ppyright © 2001 M. E. Kabay. All rights reserved.

1. Some cyberlaw sites:

Computer Law Observer <a href="http://www.lawcircle.com/observer">http://www.lawcircle.com/observer</a>

Cyberspace Law Abstracts <a href="http://www.ssrn.com/update/subscript.html">http://www.ssrn.com/update/subscript.html</a>

Cyberspace Law for Non-Lawyers

http://www.ssrn.com/update/lsn/cyberspace/csllessons.html

Cyberspace Law Institute http://www.cli.org/default.html

- 2. Cavazos, E. & G. Morin (1996). *Cyberspace and the Law: Your Rights and Duties in the On-Line World.* MIT Press (Cambridge, MA). ISBN 0-262-53123-2. 220 pp. Index.
- 3. Rose, L. J. (1994). *NetLaw: Your Rights in the Online World*. Osborne/McGraw-Hill (New York). ISBN 0-07-882077-4. xx + 372. Index.
- 4. Rosenoer, J. (1997). *CyberLaw: The Law of the Internet.* Springer-Verlag (New York). ISBN 0-387-94832-5. xiv + 362. Index.
- 5. Stephenson, P. (1999). *Investigating Computer-Related Crime: A Handbook for Corporate Investigators*. Auerbach Publications (Boca Raton, FL). ISBN 0-849-32218-9. 328 pp. Index.
- 6. Wright, B. (1996). *The Law of Electronic Commerce: EDI, E-mail and Internet -- Technology, Proof and Liability, Second Edition*. Little, Brown (Boston). ISBN 0-316-95645-7. xxxv + 471. Appendices, index.

## **Legal Issues**

- Appropriate use policies
- Cultural differences and the World Wide Web
- Intellectual property
- Due diligence
- Downstream liability
- Jurisdiction and prosecution



- 1. Kabay, M. E. (2001). "Protecting your reputation in cyberspace." See six parts in http://www.nwfusion.com/newsletters/sec/
- 2. Saudi Arabia censors the Internet to prevent images of emancipated women from threatening its cultural attitudes towards women's acceptable roles in society.
- 3. Kabay, M. E. (2000). "The Napster Cantata." The Napster cantata. <a href="http://www.securityportal.com/articles/napster20001013.html">http://www.securityportal.com/articles/napster20001013.html</a> and <a href="http://www.securityportal.com/kfiles/files/napster.html">http://www.securityportal.com/kfiles/files/napster.html</a>
- 4. Kabay, M. E. (2000). "Distributed Denial-of-Service Attacks, Contributory Negligence and Downstream Liability." (2000-02-28) <a href="http://www.acm.org/ubiquity/views/m\_kabay\_1.html">http://www.acm.org/ubiquity/views/m\_kabay\_1.html</a>

### **Overview**

- Fundamental Elements of INFOSEC
- Major challenges for information security today
- Strategic responses
- Grounds for hope
- Recommendations



### **Strategic Responses**

- Education at all levels on ethical use of computers and networks
- IPv6
- Better training for network admins
- Lawsuits against managers who tolerate poor security
- Lawsuits against organizations whose bad security provides a platform for attacks by criminals against other victims
- Centralized repository of anonymized intrusion data and all requisite configuration details.
- Mandatory reporting of computer emergencies to a centralized agency for data collection and analysis.



1.	Kabay, M. E. (2001). "Why kids shouldn't be criminal hackers, v08." <a href="http://www.securityportal.com/kfiles/files/kidcriminals.html">http://www.securityportal.com/kfiles/files/kidcriminals.html</a>

## Strategic Responses (cont'd)

- Revolt by users -- including class-action lawsuits -- to force software manufacturers to include usability and security into their products.
- Consumer boycott of software released with major flaws.
- Smart tokens or biometric authentication
- Professional vulnerability assessment services or tools to test corporate perimeters.
- Dreamtime: attack obsessive concern with quarterly bottom line that prevents sound risk management.



### **Overview**

- Fundamental Elements of INFOSEC
- Major challenges for information security today
- Strategic responses
- Grounds for hope
- Recommendations



## **Grounds for Hope**

#### Overview:

- Growing public awareness of computer crime
- Infrastructure protection growing
- Information assurance education improving
- Information sharing



### **Public Awareness**

- Growing number of articles about INFOSEC in popular press
- Distributed Denial of Service attacks (Feb 2000) led to stock-market effects
- Pump and dump scams increasing
- Online auctions major source of fraud
- Online gambling
  - Gambling: tax on poor arithmetic skills
  - Online gambling: tax on low IQ



Copyright © 2001 M. E. Kabay. All rights reserved.

- 1. RISKS 20(81): Peter G. Neumann wrote in RISKS: "A fake press release announced a merger of Aastrom Biosciences Inc. with Geron Inc., a California biopharmaceutical house. Aastrom stock fell, while Geron rose. Aastrom asserted that the message on their Website was totally bogus, and presumably the result of a penetration."
- 2. RISKS 21(06): On 20 Sep 2000, Jonathan Lebed, 15, settled a federal civil-fraud process, agreeing to pay \$272,826 for perpetuating bogus information on the Internet that led to the stock fluctuations in Just Toys Inc. and The Havana Republic and profiting therefrom.
  - NewsScan: SEC SWEEP NETS 33 FRAUDSTERS

Days after arresting the California man responsible for the Emulex hoax, U.S. Securities and Exchange Commission officials conducted its fourth major "Internet sweep," taking action against 33 companies and individuals accused of using the Internet to defraud investors in classic "pump and dump" stock scams. Enforcers cited manipulation of more than 70 microcap or penny stocks, which are more loosely regulated than Big Board shares and have long been the target of illegal trading activities. "Thinly traded microcap stocks are particularly susceptible to online manipulations," says Richard H. Walker, SEC director of enforcement. "That's why we have made this area one of our highest enforcement priorities." The individuals and companies charged on Wednesday had allegedly reaped illegal profits totalling more than \$10 million. Many of the individuals had no experience in stock trading, and included a bus mechanic, a college student and a car-service driver. (Financial Times 7 Sep 2000)

-	
-	
-	
_	

## **Business Development, Not Just Loss Avoidance**

- Traditional view of security:
  - Loss avoidance
- Competitive e-commerce marketplace
  - Consumer concerns over privacy
  - Significant portion of population do not trust the Internet
- Bricks-and-mortar businesses also involved
  - Specific contract (distributor, Chicago) where clients refused to do business
  - Needed security assessment/improvement to regain confidence of major clients



Committee 2001 M. F. Kahan. All rights reserved

- 1. Worstell, K., M. Gerdes & M. E. Kabay (2000). Net present value of information security. http://securityportal.com/cover/coverstory20001023.html
- 2. **Defining the Net Present Value of Information Security** from a draft White Paper by M. E. Kabay (unpublished)

Tom Nelson, VP and Chief Strategy Officer of AtomicTangerine has defined the Net Present Value of Information Security (NPVSec) as follows: "NPVSec is the value protection and value creation that is realized when barriers to e-Business are removed through mechanisms that ensure business integrity, service availability and customer/consumer confidentiality and privacy. Value creation examples include: new distribution channels, new revenue streams, new business models, among others."

In other words, instead of viewing information security solely as a risk-avoidance measure — like a kind of insurance policy that never actually pays anything back — we are forced by the nature of e-business to accept that security actually *supports* and *enables* e-business.

As we have seen in our review, e-business has brought security to the forefront of strategic thinking for successful businesses. Business leaders can no longer tolerate the view that security is an add-on feature relegated to the end of the design process. Security is a process, not a product or a state; security affects every e-businesses bottom line in a positive way. Security is no long a cost center, it's part of your repertoire for meeting the legitimate needs of your public. Instead of seeing security as solely the purview of the technical staff in your organization, you should ensure that your marketing and public relations departments are well versed in the principles of information security and can communicate effectively to an anxious public about the measure you are taking to safeguard your customers' privacy and their money. Be sure that your Web site has clear and appropriate privacy policies; don't sell or trade visitors' and customers' information without their explicit opt-in permission.

Secure your systems and you will secure your future.

# **Infrastructure Protection Growing**

- 1996: InfraGard
  - Cleveland FBI office started project
  - NIPC provided support starting 1998
- 1997: Report of the President's Commission on Critical Infrastructure Protection
- **1998**:
  - National Infrastructure Assurance Partnership (NIAP)
  - National Infrastructure Protection Center (NIPC)
- 2001: 2001 all 56 FBI Field Offices have chapter of InfraGard



http://www.infragard.net/
http://www.info-sec.com/pccip/web/
http://niap.nist.gov/
http://www.nipc.gov/

# **Information Assurance Education**

- INFOSEC graduates receiving excellent salaries
  - \$65,000 for BSc
  - \$85,000 for MSc
  - \$110,000 for PhD
  - (Full Professor \$80,000 "eating our seed corn")
- NSA NIETP: National INFOSEC Education and Training Program
  - Centers of Academic Excellence in Information Assurance Education
  - 23 universities listed so far

Grants to put industry experts on faculty

seminars and events

1.	Centers Of Academic Excellence In Information Assurance Education are designated by the US National Security Agency (NSA); see <a href="http://www.nsa.gov/isso/programs/coeiae/index.htm">http://www.nsa.gov/isso/programs/coeiae/index.htm</a> for details of the National INFOSEC Education and Training Program (NIETP).
2.	See the following pages for a proposal on solving this problem.
_	
_	

### News from the Front

#### TIME FOR INDUSTRY TO SUPPORT ACADEMIC INFOSEC

By M. E. Kabay, PhD, CISSP

Security Leader, INFOSEC Group, AtomicTangerine, Inc.

Copyright © 2001 M. E. Kabay. All rights reserved.

In October 2000, Dr Eugene Spafford was given the NCSC (National Computer Security Center) Achievement Award for 2000 at the 23rd NISSC (National Information Systems Security Conference) in Baltimore. In his plenary address, Dr Spafford stated that universities are unable to compete with the salaries available to students graduating from INFOSEC programs. "We are eating our seed corn," said Dr Spafford.

The reality of that statement hit me forcibly a few weeks ago when I was discussing salaries at a university where I will soon be an Associate Professor. A Full Professor – the top rank in the teaching hierarchy – earns a maximum salary of \$65,000. That's easily less than one third of the income such experts could earn in an equivalent industry position in research, development, and consulting. Some private universities can pay more, but not by much compared with the much wider range of salaries in industry.

Apologists for the low salaries claim that academics work only part of the year; however, all the professors I know work hard to stay up to date and to write papers and books.

Even the pay for Adjunct instructors – often drawn from industry – is below par. For example, the university where I will teach pays \$50 per contact hour (and nothing for preparation time, grading or help to students). Put these fees in context by recalling that in contrast, commercial teaching organizations typically pay instructors \$1,000-\$1,500 a day and those of us with higher demand for our time charge several times that (e.g., my fee for a one day course is currently \$7,000 plus expenses and travel time).

We are making a mistake by underpaying our academic colleagues. Teachers play much the same role in society as a valve does in a hydraulic system: they control the flow in the process. Without teachers we suffer from inadequate supply of security specialists -- as many recent news stories about the state of INFOSEC will attest.

The blinkered response of industry to the shortage of security specialists has been to increase salaries -- the classic supply/demand reaction. Free-market ideologues insist that the market value of a university degree in INFOSEC should rise accordingly, much as the price of a medical degree or of an MBA is higher than the price of a Baccalaureate at the same university. With the rise in revenue from students should come an increase in salaries for professors to teach those courses -- or so the theorists would have us believe.

Alas, it's not so simple. Student fees are only one component of revenue for academic institutions and faculty salaries are certainly not the only drain. Because money is fungible, ideal market forces are unable to influence faculty salaries directly.

The other problem is that we are in stuck in a stable-unsatisfactory social-feedback system (otherwise known as a Catch-22). Low faculty salaries contribute to the paucity of students trained in INFOSEC and therefore to higher salaries for those graduates who are so trained – and so the gap between faculty salaries and industry salaries grows.

What about government intervention? Recent announcements of funding for Centers of Excellence in INFOSEC training will certainly help specific institutions. However, getting the grants depends in some measure on having established programs and qualified faculty, which in turn depend in part on getting the grants – another Catch-22.

So where does all this leave us?

(Cont'd on next page)

### News from the Front

(Cont'd from previous page)

I think industry ought to fund endowed chairs at many universities for INFOSEC studies. An endowed chair draws a professor's salary in part from the interest on donated capital. Taking a conservative estimate of 5% return on investment and a generous allowance of 1% to be kept back to compensate for currency inflation, we could fund a \$150,000 salary for a professor of INFOSEC with an endowment of \$3,750,000. True, this amount wouldn't cover ancillary expenses and mandatory contributions to university overhead, but it would be a start.

Such a sum may seem astronomical to wage-earning peons like me (and perhaps most of my readers) but it is in the range of salaries and bonuses paid to quite a few top executives. Let's not even get into the question of baseball players <g>, some of whom have recently gotten contracts in the tens of millions of dollars per year.

Perhaps only a few of the very largest corporations or the wealthiest individuals could afford such donations as a single payment, partly because shareholders and employees might object. However, there is nothing to stop businesses from banding together to contribute collectively to such a project.

I suggest that INFOSEC organizations promote nationwide fund-raising drives to endow chairs at suitable institutions. These organizations would probably not be able to supply funds themselves, but they could provide invaluable volunteer-power to canvass their members' employers.

Some respected candidate organizations – both non-profit and for-profit – include (in no particular order) the Information Systems Security Association (ISSA), the International Information Systems Security Certification Consortium (ISC)^2, the Computer Security Institute, the MIS Training Institute, the High-Technology Crime Investigation Association (HTCIA), and various vendor consortia of ICSA Labs; and security subgroups in technology associations such as the Information Technology Association of America (ITAA), the Institute of Electrical and Electronic Engineers (IEEE), the Association for Computing Machinery (ACM) and various platform-specific associations such as the HP-oriented INTEREX and the Digital-Equipment-centered DECUS. Members of other bodies will surely want to get involved.

All of these organizations have either volunteer members or paying clients who are loyal to the aims and services provided. Some have corporate members who might be interested in supporting endowments. Most important, all of the people and organizations can go into their business and personal communities and look for funding not only from vendors in the INFOSEC arena but even in the wider community affected by the lack of enough INFOSEC teachers and researchers. Banks, e-commerce businesses (those that haven't failed in the market downturn), telecommunications companies, Internet service providers, manufacturers, insurance companies, transport companies, even health-care organizations – all these enterprises would benefit from an improved supply of trained information-security graduates.

If anyone is interested in working towards such a project, contact me and I will put volunteers in touch with each other. Write to me at mkabay@atomictangerine.com with your comments and suggestions.

This paper may be freely reprinted provided it is intact and includes the copyright statement and this permission statement.

## **Information Sharing**

- InfraGard
- Vulnerability databases
- Industry consortia
- Alert services



- 1. Contact your local FBI field office to get information about InfraGard.
- 2. See the ICAT Metabase for a searchable database of known vulnerabilities and exposures at <a href="http://icat.nist.gov/icat.cfm">http://icat.nist.gov/icat.cfm</a>
- 3. ICSA Labs organizes several INFOSEC industry consortia; see <a href="http://www.icsalabs.com/">http://www.icsalabs.com/</a>
- 4. AtomicTangerine organizes the International Institute for Information Integrity (I-4); see <a href="http://www.atomictangerine.com/i-4.htm">http://www.atomictangerine.com/i-4.htm</a>
- 5. CERT-CC is one of the most important sources of information about evolving vulnerabilities; see <a href="http://www.cert.org">http://www.cert.org</a>
- 6. See the following pages for other INFOSEC resources.

•		

#### News from the Front

#### Some Useful INFOSEC Publications.

Some paper publications are listed below:

- Computer Security Alert (monthly) and Computer Security Journal (quarterly). Both are benefits of membership in the Computer Security Institute) <a href="http://www.gocsi.com">http://www.gocsi.com</a> and http://www.gocsi.com/excerpt.htm (editorial archives)
- INFOSECURITY News Magazine (free) <a href="http://www.scmagazine.com">http://www.scmagazine.com</a>
- Information Security Magazine (free) <a href="http://www.infosecuritymag.com/">http://www.infosecuritymag.com/</a>
- SC Information Systems Security (\$175/year for six issues) Auerbach Publications http://www.auerbach-publications.com/contents/issad.htm

Some useful electronic publications that cover information security news which you can receive by e-mail (free unless otherwise noted) include the following (pointers to subscription information are given wherever possible):

- ACM TechNews includes security news as well as general information industry news (thrice weekly; free to ACM members) <a href="http://www.acm.org/technews/">http://www.acm.org/technews/</a>
- Benton Project Communications-related Headlines (daily) <a href="http://www.benton.org/News/">http://www.benton.org/News/</a>
- Bugtraq (see subscription form in frame on) <a href="http://www.securityfocus.com/">http://www.securityfocus.com/</a>
- CERT-CC Advisories and Summaries <a href="http://www.cert.org/contact\_cert/certmaillist.html">http://www.cert.org/contact\_cert/certmaillist.html</a>
- EDUPAGE http://listserv.educause.edu/cgi-bin/wa.exe?SUBED1=edupage&A=1
- FindLaw's DOWNLOAD THIS! A Weekly Newsletter Covering Law and the Internet http://my.findlaw.com
- Help Net Security (weekly) <a href="http://www.net-security.org/text/newsletter/">http://www.net-security.org/text/newsletter/</a>
- Network World Fusion's Security Newsletter (twice weekly tutorials and articles by MK) http://www.nwfusion.com/newsletters/sec/
- Pete Moss Publications -- newsletters about Spam, Security, MP3, E-Commerce, Privacy, Viruses and Censorship <a href="http://petemoss.com/">http://petemoss.com/</a>
- POLITECH (daily) moderated by Declan McCullagh http://www.politechbot.com/info/subscribe.html
- RISK Forum Digest (irregular) moderated by Peter G. Neumann http://www.CSL.sri.com/risksinfo.html
- SANS NewsBites mailto:sans@sans.org with the subject: Subscribe NewsBites
- SearchSecurity Newsletter (daily)
   <a href="http://searchsecurity.techtarget.com/searchSecurity\_Member\_Benefits\_Page/0,282323,1,0">http://searchsecurity.techtarget.com/searchSecurity\_Member\_Benefits\_Page/0,282323,1,0</a>
   0.html
- Security Intelligence News Service (weekly) <a href="http://dso.com/cgi-bin/dsoindex.cgi/?cartid=983070559&next=newsletter.html">http://dso.com/cgi-bin/dsoindex.cgi/?cartid=983070559&next=newsletter.html</a>
- SecurityPortal (weekly) newsletters on BSD, CheckPoint, Linux, Microsoft, General Security News, PGP, Raptor, Solaris, Tools, and Viruses <a href="http://listserv.securityportal.com/SCRIPTS/WA-SECURITYPORTAL.EXE?SUBED1=securityportal-l&A=1">http://listserv.securityportal.com/SCRIPTS/WA-SECURITYPORTAL.EXE?SUBED1=securityportal-l&A=1</a>
- Security Wire Digest (twice weekly) from Information Security Magazine http://infosecuritymag.industryemail.com

### News from the Front

As for finding further information about information security, I suggest the following Web sites as good starting points (in addition to several of the sites mentioned above, which have daily news updates online):

- CERIAS Hotlist <a href="http://www.cerias.purdue.edu//hotlist/">http://www.cerias.purdue.edu//hotlist/</a>
- CERT/CC articles, reports & papers <a href="http://www.cert.org/nav/allpubs.html">http://www.cert.org/nav/allpubs.html</a>
- ICAT Metabase (search engine for CVE -- Common Vulnerabilities and Exposures -- Database) http://icat.nist.gov/icat.taf
- ICSA Labs / Trusecure Corporation's Hype or Hot index http://www.trusecure.com/html/tspub/hypeorhot/index.shtml
- Information Security Resources <a href="http://security.isu.edu/">http://security.isu.edu/</a>
- Information Security University <a href="http://www.infosecu.com">http://www.infosecu.com</a>
- InfoSec and InfoWar Portal <a href="http://www.infowar.com/">http://www.infowar.com/</a>
- INFOSYSSEC, a truly awesome collection of links, news and search engines http://www.infosyssec.com/infosyssec/index.html
- International Computer Security Laws <a href="http://www.mossbyrett.of.no/info/legal.html">http://www.mossbyrett.of.no/info/legal.html</a>
- Network/Computer Security Technology <a href="http://jotruitt.home.mindspring.com/sectech/">http://jotruitt.home.mindspring.com/sectech/</a>
- Security and Cryptography links <a href="http://www.semper.org/sirene/outsideworld/security.html">http://www.semper.org/sirene/outsideworld/security.html</a>
- SecurityFocus <a href="http://www.securityfocus.com/">http://www.securityfocus.com/</a>
- SecurityPortal <a href="http://www.securityportal.com">http://www.securityportal.com</a>
- TechRepublic configurable Web pages (browse by topic or sign up using link on) <a href="http://www.techrepublic.com">http://www.techrepublic.com</a>

### **Overview**

- Fundamental Elements of INFOSEC
- Major challenges for information security today
- Strategic responses
- Grounds for hope
- Recommendations



Convright © 2001 M. F. Kahav. All rights reserved.

- 1. This section is *not* intended to provide technical details. It will serve to alert participants to some of the key areas where management needs to support information technology and security professionals.
- 2. One of the most useful summaries of responses to key technical threats and vulnerabilities is the SANS Institute's *How to Eliminate the Ten Most Critical Internet Security Threats: The Experts' Consensus* which is regularly updated. Version 1.32 (2001-01-18) is available at <a href="http://www.sans.org/topten.htm">http://www.sans.org/topten.htm</a>

•	

### Recommendations

#### Overview

- Establish sound security policies
- Design security architecture around policies
- Partition your information space
- Keep your systems up to date
- Test your perimeter defenses
- Use intrusion-detection systems
- Implement effective monitoring and enforcement
- Plan for incident response
- Cooperate in the fight against DoS
- Apply social psychology to security



Copyright © 2001 M. E. Kabay. All rights reserved.

Some more advanced resources for learning about information and network security:

BSI (1997). *IT Baseline Protection Manual: Recommended Measures to meet Medium-Level Protection Requirements*. Prepared by the Bundesamt für Sicherheit in der Informationstechnik of the German Federal Government. English version at <a href="http://www.bsi.bund.de/gshb/english/menue.htm">http://www.bsi.bund.de/gshb/english/menue.htm</a>

Ford, W. & M. S. Baum (1997). *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption.* Prentice Hall (Upper Saddle River, NJ). ISBN 0-13-476342-4. xxv + 470. Index.

Fraser, B. (1997), ed. *Site Security Handbook.* RFC2196 (Network Working Group). <a href="http://www.cis.ohio-state.edu/htbin/rfc/rfc2196.html">http://www.cis.ohio-state.edu/htbin/rfc/rfc2196.html</a>

Garfinkel, S. & G. Spafford (1997). *Web Security and Commerce*. O'Reilly & Assoc (Sebastopol, CA). ISBN 1-56592-269-7. 483 pp. Index.

Kovacich, G. L. (1998). *The Information Systems Security Officer's Guide: Establishing and Managing an Information Protection Program*. Butterworth Heinemann (Woburn, MA). ISBN 0-7506-9896-9. xv + 172. Index.

Peltier, T. R. (1998). *Information Security Policies and Procedures: A Practitioner's Reference*. Auerbach Publications (Boca Raton, FL). ISBN 0-8493-9996-3. 250 pp, CD-ROM. \$245

Schneier, B. (2000). Secrets & Lies: Digital Security in a Networked World. Wiley (New York). ISBN 0-471-25311-1. xvii + ~400. Index.

Stallings, W. (1995). *Network and Internetwork Security: Principles and Practice*. Prentice Hall (Englewood Cliffs, NJ). ISBN 0-02-415483-0. xiii + 462. Index.

Tipton, H. F. & M. Krause (2000), eds. *Information Security Management Handbook*, 4<sup>th</sup> edition. Auerbach (Boca Raton, FL). ISBN 0-8493-9829-0. xiii + 711. Index.

## **Establish Sound Security Policies**

- Create Information Protection Working Group
  - Upper-management support
  - Respected, experienced leader
  - Representatives from every sector
- Identify key exposures
  - Sensitive data and systems
  - Critical data and systems
- Use security-policy templates to save time
  - C. C. Wood
  - T. Peltier



ppyright © 2001 M. E. Kabay. All rights reserved.

See the long series of articles published in Network World Fusion's security newsletter: Kabay, M. E. (2000) –

- Introduction to Psycho-Social Factors in the Implementation of Security Policy. (2000-02-16) <a href="http://www.nwfusion.com/newsletters/sec/0214sec2.html">http://www.nwfusion.com/newsletters/sec/0214sec2.html</a>
- Rationality is Not Enough. (2000-02-23) http://www.nwfusion.com/newsletters/sec/0221sec2.html
- Framing Reality. (2000-03-08) <a href="http://www.nwfusion.com/newsletters/sec/0306sec2.html">http://www.nwfusion.com/newsletters/sec/0306sec2.html</a>
- Getting Your Security Policies Across. (2000-03-15) <a href="http://www.nwfusion.com/newsletters/sec/0313sec2.html">http://www.nwfusion.com/newsletters/sec/0313sec2.html</a>
- Beliefs and Attitudes. (2000-03-22) http://www.nwfusion.com/newsletters/sec/0320sec2.html
- Changing Attitudes Towards Security. (2000-03-29) http://www.nwfusion.com/newsletters/sec/0327sec2.html
- Encouraging initiative. (2000-04-06) http://www.nwfusion.com/newsletters/sec/0403sec2.html
- Dirty words: Conformity, compliance and obedience. (2000-04-13). http://www.nwfusion.com/newsletters/sec/0410sec2.html
- Group behavior and security. (2000-04-20) http://www.nwfusion.com/newsletters/sec/0417sec2.html
- Tips for improving security education. (2000-04-27) <a href="http://www.nwfusion.com/newsletters/sec/0424sec2.html">http://www.nwfusion.com/newsletters/sec/0424sec2.html</a>

(Cont'd on next page)

## **Design Security Architecture Around Policies**

- Security equipment cannot protect systems effectively without good policies
- Firewalls
  - Define acceptable inbound traffic
  - Exclude everything else
  - Define acceptable outbound traffic
  - Block everything else (e.g., spoofed packets)
- Intrusion-detection systems
  - Define normal behavior
  - Prevent false-positives



Copyright © 2001 M. E. Kabay. All rights reserved.

#### (Cont'd from previous page)

- Personnel and security: Hiring. (2000-05-04)
   <a href="http://www.nwfusion.com/newsletters/sec/0501sec2.html">http://www.nwfusion.com/newsletters/sec/0501sec2.html</a>
- Personnel and security: Opportunities for abuse. (2000-05-10) http://www.nwfusion.com/newsletters/sec/0508sec2.html
- Personnel and security: Redundancy. (2000-05-17) <a href="http://www.nwfusion.com/newsletters/sec/0515sec2.html">http://www.nwfusion.com/newsletters/sec/0515sec2.html</a>
- Personnel and security: The expert in the next office. (2000-05-24) http://www.nwfusion.com/newsletters/sec/0522sec2.html
- Personnel and security: Cross-training and vacation time. (2000-05-31) <a href="http://www.nwfusion.com/newsletters/sec/0529sec2.html">http://www.nwfusion.com/newsletters/sec/0529sec2.html</a>
- Personnel and security: The thin line. (2000-06-07) http://www.nwfusion.com/newsletters/sec/2000/0605sec2.html
- Personnel and security: Separation of duties. (2000-06-14) http://www.nwfusion.com/newsletters/sec/2000/0612sec2.html
- Personnel and security: Firings and resignations. (2000-06-21) http://www.nwfusion.com/newsletters/sec/2000/0619sec2.html
- Personnel and security: How to say goodbye. (2000-06-28) http://www.nwfusion.com/newsletters/sec/2000/0626sec2.html
- Personnel and security: Psychosocial issues in firing. (2000-07-05) http://www.nwfusion.com/newsletters/sec/2000/0703sec2.html
- Security policy resources. (2000-07-19) http://www.nwfusion.com/newsletters/sec/2000/0717sec2.html

# **Partition Your Information Space**

- Prevent unauthorized access to network components
  - Firewalls
  - Network topologies
- Internal networks need protection from each other too; e.g.,
  - Human Resources records
  - Engineering data
  - Legal department
  - Finance
  - Sales . . . .



Copyright © 2001 M. E. Kabay. All rights reserved.

1.	For a	primer	on	network	topol	logy,	see
----	-------	--------	----	---------	-------	-------	-----

Guidelines and Techniques for Defining Your Network Topology from CISCO Systems.

The HTML version is at

http://www.cisco.com/univercd/cc/td/doc/product/ismg/policy/ver20/topology/nwgdlin.htm and there is a PDF version for easy printing at

http://www.cisco.com/univercd/cc/td/doc/product/ismg/policy/ver20/topology/nwgdlin.pdf

2. See also

Verstraete, A. A. (1998). Network Topology.

http://www.smeal.psu.edu/misweb/datacomm/netstopo.html

which is part of a larger course on data communications at Penn State University that starts at http://www.smeal.psu.edu/misweb/datacomm/

# **Keep Your Systems up to Date**

- CERT-CC Summaries and Alerts http://www.cert.org
- Vendor bulletins
- USENET groups
- Keep anti-virus products current
- Newsletters
- Magazines
- Conferences



- 1. For a central repository of links to information security resources on the Web, see the CERIAS Hotlist at < <a href="http://www.cs.purdue.edu/cerias/hotlist/">http://www.cs.purdue.edu/cerias/hotlist/</a>>
- 2. Another source of useful information is SecurityPortal at < <a href="http://www.securityportal.com">http://www.securityportal.com</a>
- 3. A spectacularly dense source of INFOSEC information is < <a href="http://www.infosyssec.com">http://www.infosyssec.com</a>
- 4. Take advantage of the Global Incident Analysis Center run by SANS: < http://www.sans.org/giac.htm >

•	•		

## Test Your Perimeter Defenses

- Quality assurance experience: no one can check their own products well
- Use independent outside evaluation of security
- Avoid criminal hackers or companies who hire them
- Criteria for verification should be dynamic and keep up with changing environment
- Repeatedly test perimeter: security is not a product, it's not a state: it's a continuing process.



1.	Kabay, M. E. (2000). "Social engineering simulations." (2001-12-18) http://www.nwfusion.com/newsletters/sec/2000/00292157.html
2.	Schneier, B. (1999). "Security is not a product, it's a process." Crypto-Gram (1999-12-15). <a href="http://www.counterpane.com/crypto-gram-9912.html">http://www.counterpane.com/crypto-gram-9912.html</a>
_	
_	

# **Use Intrusion-Detection Systems**

- Expect penetration and plan for it
- IDS provide early warnings of trouble
- Respond effectively and quickly
  - Capture valuable data
    - Targets
    - Tools
    - Origins
  - Maintain chain of evidence for forensic use
  - Divert attacker to honey-pot if appropriate
- Plan for prosecution as much as possible



1.	Kabay, M. E. (2000). "Intrusion Detection Resources." (2000-10-23) <a href="http://www.nwfusion.com/newsletters/sec/2000/1023sec1.html">http://www.nwfusion.com/newsletters/sec/2000/1023sec1.html</a>
2.	Bace, R. B. (1999). "An Introduction to Intrusion Detection And Assessment." <a href="http://www.icsa.net/html/communities/ids/White%20paper/index.shtml">http://www.icsa.net/html/communities/ids/White%20paper/index.shtml</a>
3.	Bace, R. B. (2000). <i>Intrusion Detection</i> . Macmillan Technical Publishing (Indianapolis, IN). ISBN 1-57870-185-6. xix + 339. Index.

# Effective Monitoring and Enforcement

- Enable audit trails (logs) wherever possible
- Post clear announcements about constant monitoring of
  - logins and logoffs
  - activity during sessions
  - e-mail
  - Web browsing
- Pay special attention to compliance by top management



1. For examples of logon banners, see						
$\underline{http://www.itsc.state.md.us/info/InternetSecurity/BestPractices/WarnBanner.html}$						
http://www.ja.net/CERT/JANET-CERT/regulation/aups.html						
http://www.fas.org/irp/congress/1996_hr/s960605d.htm						
• Codi, R. (date not provided). Welcome Banners.						
http://www.infosysnetworks.com/welcome_banners.htm						
[Note that the gaps in the underlined URL are actually underscore characters ("_").]						
3. CERT/CC (1999). Setting up a logon banner on Windows NT 4.0						
http://www.cert.org/security-improvement/implementations/i034.01.html						

## Plan for Incident Response

- Growing awareness of importance of intrusion detection
- Timely response essential in minimizing damage
- Security paradigm shifting to focus on delay sufficient to allow effective response
- Cannot invent response plans -- must be tried and honed



1.	Escamilla, T. (1998). <i>Intrusion Detection: Network Security Beyond the Firewall</i> . John Wiley & Sons (New York). ISBN 0-471-29000-9. xx + 348. Index
2.	Toigo, J. W., M. R. Toigo (1999). Disaster Recovery Planning: Strategies for Protecting Critical Information Assets. Prentice Hall (Upper Saddle River, NJ). ISBN 0-130-84506-X. 325 pp. Index.

### **Build Your Own CERT**

- Operations staff
- Programmers
- Network managers
- Telecommunications
- Public relations
- Legal department
- Human resources department
- Upper management representative
- Vendor liaison
- Law enforcement liaison



- 1. CERT/CC (2001). CSIRT [Computer Security Incident Response Team] Development. <a href="http://www.cert.org/csirts/">http://www.cert.org/csirts/</a>
- 2. West-Brown, M. (2000). *Awooding the Trial-By-Fire Approach to Security Incidents*. <a href="http://www.stsc.hill.af.mil/crosstalk/2000/oct/westbrown.asp">http://www.stsc.hill.af.mil/crosstalk/2000/oct/westbrown.asp</a>
- 3. CERT/CC (2001). Creating a Computer Security Incident Team. (Course description). <a href="http://www.cert.org/nav/training.html#csirt1day">http://www.cert.org/nav/training.html#csirt1day</a>

٠	
•	
٠	
٠	
٠	
•	



Reprinted with permission of the author, Kevin Siers. Copyright © 2000 Kevin Siers, The Charlotte Observer. All rights reserved.

See Kevin Siers' archive of editorial cartoons at <a href="http://www.charlotte.com/siers.htm">http://www.charlotte.com/siers.htm</a>

# Cooperate in the Fight Against DoS

- Use of resources for nefarious purposes
  - Can launch attacks without violating access controls
  - Saturate tables
  - Fill data communications channels
  - Lock resources
  - Melissa, Love Bug damage was from resource saturation
- Prevent infection by zombies
- Institute egress filtering at firewalls
  - Block forged packets
  - Block outbound floods



Copyright © 2001 M. E. Kabay. All rights reserved.

- 1. CISCO (2000). Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks. http://www.cisco.com/warp/public/707/newsflash.html
- 2. Paul Ferguson's DoS Resources <a href="http://www.denialinfo.com/">http://www.denialinfo.com/</a>
- 3. Dave Dittrich's DDoS Attacks/tools http://staff.washington.edu/dittrich/misc/ddos/
- 4. SANS (2000). *Help Defeat Denial of Service Attacks: Step-by-Step.* http://www.sans.org/dosstep/index.htm
- 5. Savage, S., D. Wetherall, A. Karlin & T. Anderson (2000). *Practical Network Support for IP Traceback*. http://www.cs.washington.edu/homes/savage/traceback.html
- 6. Bellovin, S. M. (2000). *Distributed Denial of Service Attacks* (presentation). http://www.research.att.com/~smb/talks/nanog-dos/index.htm
- 7. Cohen, F. (2000). Managing Network Security: Countering DCAs [Distributed Coordinated Attacks]. <a href="http://all.net/journal/netsec/0004.html">http://all.net/journal/netsec/0004.html</a>
- 8. Senie, D. (1999). *Changing the Default for Directed Broadcasts in Routers*. RFC 2644. <a href="http://www.ietf.org/rfc/rfc2644.txt?number=2644">http://www.ietf.org/rfc/rfc2644.txt?number=2644</a> or

ftp://ftp.isi.edu/in-notes/rfc2644.txt

9. Ferguson, P. (1998). *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*. RFC 2267 <a href="http://www.ietf.org/rfc/rfc2267.txt?number=2267">http://www.ietf.org/rfc/rfc2267.txt?number=2267</a> or

ftp://ftp.isi.edu/in-notes/rfc2267.txt

# **Psycho-Social Factors in Culture Change**

- Involve every department in developing INFOSEC policies
- Involve top management at all phases
- Use one-on-one sessions to gain support and champions
- Provide concrete examples of real losses from cases of computer crime or accident
- Keep productivity in mind
- Choose personality types who won't be authoritarian when enforcing security
- Use reward, not just punishment



Copyright © 2001 M. E. Kabay. All rights reserved.

Kabay, M. E. (1996). Kabay, M. E. (1996). The NCSA Guide to Enterprise Security:
Protecting Information Assets. McGraw-Hill (New York). ISBN 0-07-033147-2. xii + 388 pp. Index. See chapter 11.

## **DISCUSSION**



Copyright © 2001 M. E. Kabay. All rights reserved.

Feel free to contact me any time.

M. E. Kabay, PhD, CISSP
Security Leader, INFOSEC Group
AtomicTangerine, Inc.
255 Flood Road
Barre, VT 05641-4060

Voice: +1.802.479.7937
E-mail: mkabay@atomictangerine.com