## Credo

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

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

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

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

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

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

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

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

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

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

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

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

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

\* \* \*

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

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

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

## Rules for InfoSec Perception

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

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

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

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

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

\* \* \*

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

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

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