Resources for Creating Effective Security Policies

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

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

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

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

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

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

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

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

anyone would want to buy a paper copy when one can simply print from the PDF) by using the IEC Webstore< http://webstore.iec.ch/ > and entering the standard number (e.g., 27000) into the Search field on the upper right of the page. In addition, there's a 50% educational discount available< http://webstore.iec.ch/Webstore/webstore.nsf/0/C6B6F00BE9D89ED5C125761F0055DD41?OpenDocument > for orders submitted on academic institutional letterhead. For networked access by different numbers of users in one organization, special discounts< http://webstore.iec.ch/Webstore/webstore.nsf/0/F435E5A7A69B11E9C1257556005A62F1?OpenDocument > apply; for example, 20 users can access a document bought at only four times the individual-copy rate.

The overview of ISO/IEC 27000:2009 is available free in English from < http://standards.iso.org/ittf/PubliclyAvailableStandards/c041933_ISO_IEC_27000_2009.zip > which contains a 26 page summary of most of the 27000 series of standards (those that existed as of 2009).

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

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

Additional standards in the series include

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

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

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

COBIT 5 is the forthcoming new version:

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

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

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

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

Class notes on Chapter 44, "Security Policy Guidelines," from the *Computer Security Handbook*, 5th edition< http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529/ >, are freely available in PPTX< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch44_security_policy_guidelines.pptx > and PDF< http://www.mekabay.com/courses/academic/norwich/is342/is342_lectures/csh5_ch44_security_policy_guidelines.pdf >.

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

* * *

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

* * *

Web site in accordance with the terms of the Agreement in force between *InfoSec Reviews* and M. E. Kabay.