
In my courses on the management of information assurance (IA) <http://www.mekabay.com/courses/academic/norwich/is342/index.htm> I make a point of telling my students that as managers, we should always be prepared to answer the following two questions from upper management about our proposed budgets for IA:

1. Why do we need to spend _so much money_ on IA?
2. If IA is so important to us, why aren’t you asking for _more_ money than this?

These questions focus on the idea that it should be possible to decide on optimal security expenditures for a specific organization using reason.

Before delving into the text, I want to be sure that readers are aware of a great divide in the world of security management: a battle between extreme proponents of quantitative risk management methodologies and those who insist that only qualitative methods have any validity. Personally, I like using both approaches and will discuss my position after reviewing the textbook.

Drs Gordon and Loeb began their text with a well-written review of the importance of IA in their introductory chapter. They review the evolution of management structures, the growing acceptance of security standards, and the rise of organizations supporting IA. Most important, they directly confront fundamental difficulty faced by those proposing quantitative risk management for security-related decisions: the argument that such quantitative methods are based on an incomplete and necessarily faulty base of numerical information about the costs and probabilities of security incidents. They warn that basing economic decisions about IA solely on best practices cannot guarantee that these spending levels are optimized. As they write,"... if all firms take this approach, all firms may be either overspending for security or leaving themselves open to unnecessary risks. ... Herd behavior may feel good and have some merit, but it is no substitute for carefully conducted analysis." The authors argue that both methodologies have their place.

The authors throw down the gauntlet to extreme supporters of qualitative risk analysis and management (those who deny any role to quantitative methods): “... an important goal of this book is to debunk the five cybersecurity myths listed here[:]

Myth 1: Cybersecurity activities do not lend themselves to cost-benefit analysis.
Myth 2: All cybersecurity breaches have a significant economic impact on organizations.
Myth 3: Determining the right amount to spend on cybersecurity activities is a crapshoot.
Myth 4: The role of risk management in cybersecurity is well understood.
Myth 5: Information sharing has reduced cybersecurity-related problems.

In my next column, I’ll be looking at Chapter 2: “A Cost-Benefit Framework for Cybersecurity.”

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.msia.norwich.edu> at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2006 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.