
Chapter 2 is entitled “A Cost-Benefit Framework for Cybersecurity” begins with clarification of the distinction between operating costs and capital investments -- a touchy subject for a countenance because, as the authors point out, our rapidly-changing technical and threat environments mean that much of what we buy has to be replaced relatively quickly. From some standpoints, it would make much more sense to regard IA expenditures as operating expenses; the authors write, “the fact that corporate balance sheets usually do not explicitly report cyber security investments, even though such investments are critical assets for organizations operating in the digital economy, supports the observation that firms generally expense cyber security investments.” They add, “Indeed, a good way to view all costs related to cybersecurity activities is to think of them as capital investments with varying time horizons. . . . This is the approach we take in this book.”

Next, the authors define the principles of cost-benefit analysis; in essence, “. . . the organization should keep increasing its security activities as long as the incremental benefits from increased in such activities exceed the incremental cost of those activities.” They then discuss the net present value (NPV) model, which takes into account the costs of investments over time (e.g., the costs of financing and a lost investment opportunities) and values such as loss avoidance and the incremental gains associated with those benefits -- all expressed in constant currency values. They explain the internal rate of return (IRR) and return on investment (ROI) and then provide detailed scenarios and calculations to help readers get used to these quantitative concepts.

Chapter 3, “The Costs and Benefits Related to Cybersecurity Breaches,” explores how managers can classify and evaluate direct and indirect costs as well as explicit and implicit costs. These two dimensions are orthogonal (independent). Direct costs can be traced to specific security incidents where as indirect costs include IA overhead such as firewalls and other security devices or personnel costs for IA teams. Explicit costs are those tied specifically to IA; implicit costs include consequential damages such as opportunity costs. The authors discuss the uncertainty of cost estimation and referred to research they have conducted and published on these matters. Their findings suggest” . . . that it is a myth to assume that all cybersecurity breaches have a significant economic impact on organizations. . . . However, the cybersecurity breaches associated with confidentiality do indeed tend to have a significant economic impact on organizations.”

Next time, I’ll finish this extended review of Profs Gordon and Loeb’s text as they discuss “The Right Amount to Spend on Cybersecurity” and how to talk to upper management about the value of IA.

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.