MANAGING CYBER-SECURITY RESOURCES

A COST-BENEFIT ANALYSIS

LAWRENCE A. GORDON
AND
MARTIN P. LOEB

McGraw Hill

MANAGING CYBERSECURITY RESOURCES

A Cost-Benefit Analysis

Lawrence A. Gordon
and
Martin P. Loeb

McGraw-Hill
New York Chicago San Francisco Lisbon London Madrid Mexico City
Milan New Delhi San Juan Seoul Singapore Sydney Toronto

The McGraw-Hill Companies

2 3 4 5 6 7 8 9 0 DOC/DOC 0 9 8 7

ISBN 0-07-145285-0

Library of Congress Cataloging-in-Publication Data

Gordon, Lawrence A.

Managing cybersecurity resources : a cost-benefit analysis / by Lawrence A. Gordon and Martin P. Loeb.

p. cm.

Includes bibliographical references and index.

ISBN 0-07-145285-0 (hardcover : alk. paper) 1. Business—Data processing—Security measures. 2. Computer security. 3. Information technology—Security measures. 4. Data protection. I. Loeb, Martin, P. II. Title.

HF5548.37.G67 2005

658.4'78—dc22

2005014300

PREFACE

HOW CAN MANAGERS determine the optimal level of funding for information and computer system security? How should these funds be allocated among competing cybersecurity projects? How can chief information security officers (CISOs) develop an effective business case for cybersecurity projects? These questions, which are central to this book, were among the first questions we addressed at the beginning of the millennium when we began our research on the economic aspects of cybersecurity. More to the point, the primary objective of this book is to present a framework to assist organizations in determining the appropriate amount to spend on cybersecurity activities and to efficiently allocate such resources. This framework is based on the principle of cost-benefit analysis. To our knowledge, this is the first book to provide such a framework.

As business school professors with backgrounds in managerial economics and decision support information systems, we have always had a keen professional interest in the value and use of information for managerial decision making. However, over the last decade, it has become clear to us that the rapid growth of information technology (IT) in general, and specifically the Internet, demands that our teaching and research agendas be transformed to reflect the realities of the digital economy. Chief among these realities is the growing importance of cybersecurity.

There is a rapidly emerging general realization by those working in information technology, as well as senior management (e.g., chief executive officers and chief financial officers), that the economic aspects of information security must be placed on an equal footing with the technical aspects of protecting computer networks. However, there is much confusion with respect to economic and financial concepts as applied to cybersecurity resource management. For example, the numerous articles on rates of return on information security investments appearing in a variety of professional magazines are frequently contradictory and error-prone—seemingly oblivious to the long-standing literature in accounting, economics, and finance.

This book is intended to provide a sound guide for managers dealing with the economic and financial aspects of information security. As such, this book should be a valuable resource for information security managers, financial managers responsible for the allocation of cybersecurity dollars, and other IT personnel involved in the budgeting aspects of organizational resources associated with information security. This book is also intended for use in university courses, both at the graduate and at the advanced undergraduate levels, covering the economic and financial aspects of information security.

This book does not assume any previous background in economics or information security on the part of the reader. However, some material in Chapters 2 and 4 requires a moderate degree of mathematical sophistication. Readers can skim the mathematics in these chapters and still understand the main message.

The plan of the book is as follows. In the first chapter, we discuss the importance of cybersecurity and consider some of the key issues that affect the process of managing cybersecurity resources. The second chapter provides an economic framework for managing cybersecurity resources. This framework is based on the prin-

ciple of cost-benefit analysis. The third chapter discusses cost concepts and empirical evidence related to assessing the actual costs and benefits of cybersecurity breaches. Determining the right amount to spend on cybersecurity is the subject of the fourth chapter. The fifth chapter discusses the role that risk plays in the allocation of cybersecurity resources. Chapter 6 provides a generic business case approach for securing the funding deemed necessary. Cybersecurity auditing is the subject of the seventh chapter. Chapter 8 examines the role of cybersecurity in national security, and the final chapter provides some concluding comments related to important cybersecurity issues.

ABOUT THE AUTHORS

Lawrence A. Gordon, Ph. D., is the Ernst & Young Alumni Professor of Managerial Accounting and Information Assurance and the director of the Ph.D. program at the Robert H. Smith School of Business. He is also an affiliate professor in the University of Maryland Institute for Advanced Computer Studies. Dr. Gordon earned his Ph.D. in Managerial Economics from Rensselaer Polytechnic Institute. An internationally known scholar in the area of managerial accounting and information security, Dr. Gordon's current research focuses on the economic aspects of information security, corporate performance measures, capital investments, and cost management systems. He is the author of more than 85 articles, published in such journals as *ACM Transactions on Information and System Security, Journal of Computer Security, The Accounting Review, Journal of Financial and Quantitative Analysis, Accounting Organizations and Society, Journal of Accounting and Public Policy, Decision Sciences, Omega, Journal of Business Finance and Accounting, Accounting and Business Research, Managerial and Decision Economics, Communications of the ACM,* and *Management Accounting Research.* Dr. Gordon also is the author of several books, including *Managerial Accounting: Concepts and Empirical Evidence* and *Capital Budgeting: A Decision Support System Approach.* In addition, he is the editor-in-

chief of the *Journal of Accounting and Public Policy* and serves on the editorial boards of several other journals. In two recent studies, Dr. Gordon was cited as being among the world's most influential/productive accounting researchers. Dr. Gordon is also one of the pioneers in conducting research in the area of cybersecurity economics.

An award-winning teacher, Dr. Gordon has been an invited speaker at numerous universities around the world, including Harvard University, Columbia University, University of Toronto, London Business School, and London School of Economics. He also has served as a consultant to several private (e.g., IBM) and public (e.g., U.S. Government Accountability Office) organizations. Dr. Gordon's former Ph.D. students are currently distinguished faculty members at such universities as Stanford University, Ohio State University, Michigan State University, McGill University, The College of William and Mary, University of Southern California, and National Taiwan University. His former M.B.A. students frequently call him on the "Management Accounting Hotline" (as affectionately named by his students) to discuss issues confronting their organizations. Dr. Gordon also is a frequent contributor to the popular press (e.g., *Wall Street Journal, BusinessWeek, USA Today,* and *Financial Times*). For more information about Dr. Gordon, go to his Web site at the University of Maryland (http://www.rhsmith.umd.edu/faculty/lgordon/).

Martin P. Loeb, Ph. D., is a professor of Accounting and Information Assurance and a Deloitte & Touche Faculty Fellow at the Robert H. Smith School of Business, University of Maryland, College Park. He is also an affiliate professor in the University of Maryland Institute for Advanced Computer Studies. Dr. Loeb earned his Ph.D. in Managerial Economics and Decision Sciences from the Kellogg School of Management, Northwestern University. Before embarking on research concerning the economic aspects of information security, Professor Loeb was an early leader in research on mechanism design and incentive regulation that has had a broad

impact on the fields of economics, computer science, accounting, and political science. His research on cost allocations and budget-based procurement contracting has also been influential.

Dr. Loeb's research papers have appeared in a variety of leading academic journals, including *ACM Transactions on Information and System Security, The Accounting Review, American Economic Review, Contemporary Accounting Research, Journal of Accounting Research, Journal of Banking and Finance, Journal of Computer Security, Journal of Law and Economics, Journal of Public Economics, Management Accounting Research, Managerial and Decision Economics,* and *Management Science.* Professor Loeb is an editor of the *Journal of Accounting and Public Policy* and serves or has served on the editorial boards of *The Accounting Review, British Accounting Review, Journal of Business Finance and Accounting,* and *Review of Accounting Studies*. For more information about Dr. Loeb, go to his Web site at the University of Maryland (http://www.rhsmith.umd.edu/faculty/mloeb/). Dr. Loeb is also one of the pioneers in conducting research in the area of cybersecurity economics.

Contents

CHAPTER 1

INTRODUCTION

Let's face it; when you cease to dream, you cease to live.

—ROBERT H. SMITH (BUSINESSMAN AND PHILANTHROPIST)[1]

ARE YOU WORRIED about the security of the information stored in your home and office computers? Are you worried about the security of the organizations that hold your personal, financial, and medical information? If not, you should be worried—or at least concerned.

Every day, individuals and organizations become victims of information security breaches that have significant financial implications. Indeed, the Internet revolution continues to generate new opportunities for savvy criminals to infiltrate computer systems.

[1] Taken from a speech delivered by Robert H. Smith on February 3, 2005, at a ceremony announcing his $30 million gift to the University of Maryland.

These infiltrations are what we refer to as breaches in cybersecurity. To gain peace of mind and prevent future breaches, most individuals and organizations take steps to implement some level of cybersecurity. However, given the unpredictable nature of these breaches, cybersecurity decisions are often based on gut instinct rather than on sound economic analysis. In order to rectify this situation, this book presents guidelines for efficiently managing cybersecurity resources within organizations.[2] These guidelines are based on the economic principle of cost-benefit analysis.[3]

The Internet revolution

The *Internet* is an electronic communications network that connects computers around the world and is truly the result of some big-time dreaming by several creative people. Like most great inventions, the Internet (as we know it today) evolved over time. This evolution is described by the Internet Society (2003).

In the last decade, we witnessed an unprecedented information and technological explosion led by the Internet revolution. This interconnectivity changed the way people work and play, and, in essence, the way they think about life. People now use the Internet to keep in touch with family and friends, shop online, research legal and medical questions, and entertain themselves. The Inter-

[2] Cybersecurity resources include human resources. Thus, the allocation of security resources includes the allocation of resources for the hiring and training of employees to strengthen the organization's information security. While such resource allocation falls within the scope of this book, the book does not deal with how best to manage the employees who are actively engaged in information security activities. Moreover, while the focus of this book is on managing cybersecurity resources within organizations, nearly all of the discussions could also apply to managing cybersecurity resources for individuals.

[3] Anderson (2001) argues that one needs to view information security problems from an economics perspective. This theme is also developed in Gordon and Loeb (2001b).

net also changed the way organizations operate. For example, the Internet allows employees to work from practically any location. In addition, it allows organizations to make direct purchases from vendors and to sell to customers from around the world in real time (i.e., instantaneously).

For an organization or an individual, the benefits and costs of using the Internet are largely associated with *network externalities,* or spillovers to a user of the network resulting from the fact that many others are using the same network. Benefits from network externalities are the positive spillovers to a user of the network resulting from the fact that many others are also using the same network. For example, the fact that you can connect your individual computer to the same network used by your banks, your employer, and your friends greatly increases the value of being connected to this network. The phenomenal rate of growth of the Internet in the late 1990s was largely due to such positive network externalities—as more individuals and organizations connected to the Internet, it became more attractive for others to also get connected.

While the benefits of the Internet are numerous, the Internet also creates some significant costs. One such cost, which has already wreaked havoc on countless individuals and organizations, is related to cybersecurity breaches. Computer *viruses* (malicious computer programs that cause malfunctions in a computer system), identity theft, and corporate espionage are among the best-known cybersecurity breaches. Viruses like "MyDoom" and "Code Red" can shut down thousands of computers in a matter of minutes. The costs associated with such viruses have been estimated to be in the billions of U.S. dollars, when aggregated across all of the organizations and individuals affected by these viruses.

The daily newspapers frequently include stories of cybersecurity breaches that have potentially devastating effects on organizations

and individuals. For example, on March 15, 2005, the *Wall Street Journal* ran a thought-provoking story concerning identity theft affecting hundreds of thousands of customers of several major organizations.[4]

One major reason for the proliferation of cybersecurity breaches is that the Internet was not designed with security in mind. As noted by Gansler and Lucyshyn (2004, p. 2), "[T]he Internet was designed to share information, not protect it." Recent surveys show that attacks via the Internet are the fastest-growing method of computer crime. In fact, breaches in cybersecurity have been rising at an alarming rate over the past two decades. According to the CERT Coordination Center, which has been collecting data on *security incidents* (events that compromise security) since 1988, the number of security breaches has increased dramatically since 1998.[5] For example, in 1998, CERT reported 3,734 security-related incidents, while in 2003, the number was 137,529.[6] These numbers, however, are only the tip of the iceberg because many, if not most, security breaches are never reported. Additionally, a large number of security breaches go undetected. Equally alarming are the costs associated with cybersecurity breaches. These costs are of both an explicit and an implicit nature.

Business and government leaders now recognize the significance of the frequency and costs of cybersecurity breaches. Today, cybersecurity is at the forefront of discussions about the Internet.

[4] See Saranow and Lieber (2005).

[5] Data are from CERT Coordination Center (2004).

[6] Although the CERT definition of a security incident used to generate these numbers has included intrusion attempts on computer systems via the network, there seems to be growing agreement among security professionals that intrusion attempts by themselves do not constitute a security breach.

In early 2004, Microsoft offered a $250,000 reward for information leading to the arrest and conviction of the author of the "MyDoom" computer virus. The magnitude of this reward indicates the scope and seriousness of the problem.

The cost of information security is essentially a negative network externality associated with the Internet.[7] This negative network externality arises when malevolent individuals and organizations join the network, thereby imposing costs on all well-intentioned users. These costs take the form of losses caused by actual security breaches plus the costs of actions (such as purchasing and installing antivirus software) designed to prevent such breaches. For example, the BBC news reported that the cost of the "Code Red" virus in 2001 was estimated to exceed $1.2 billion.[8]

Notice, however, that when an organization installs antivirus software, the newly installed software provides positive spillover effects to the other users of the network. That is, other users of the network receive some of the benefits when one user reduces the likelihood of spreading a virus across the network.

Information value and its link to security

Information provides value to organizations in numerous ways—by helping managers make better production, marketing, and financing decisions; by helping managers control activities and processes; and by helping to manage the workforce. In today's knowledge-based

[7] Camp and Wolfram (2000) liken negative information security externalities to pollution.

[8] See http://news.bbc.co.uk/1/hi/business/1468986.stm.

economy, information assets are replacing physical assets as a means of giving one organization a competitive advantage over another in the marketplace. Given the strategic nature of information, organizations must safeguard this asset as they would physical assets.

Protection of information is essential for facilitating normal day-to-day transactions related to buying and selling in today's digital economy. In order to conduct electronic transactions, digitized information concerning prices, product specifications, and purchasers' payment information must be securely, as well as easily, transmitted. All the e-business models—business-to-business (B2B), business-to-consumer (B2C), and business-to-government (B2G)—rely on the secure transmission and storage of sensitive information. It is essential to establish trust so that buyers and sellers are willing to participate in electronic transactions. Even firms that make all of their sales in traditional brick-and-mortar stores rely increasingly on e-commerce to manage their supply chains. Moreover, at traditional stores, sales personnel enter credit card information into the firm's computer system and electronically transmit this information to banks and credit card companies. Hence, secure information plays a valuable role in nearly all types of day-to-day business transactions.

In addition to information related to normal day-to-day business transactions, wide ranges of other types of information are key strategic assets in today's organizations. Such strategic information includes, but is not limited to, information on secret recipes, products under development, marketing plans, mergers and acquisitions, personnel, and customer demographics. Clearly, such strategic information is crucial to an organization's viability and growth. The value of this information to an organization is inextricably tied to its level of privacy and security.

Organizations typically collect information from other parties based on the understanding that the organization will protect the confidentiality of the information. This is particularly true of financial and medical information. Legal liability and compliance with laws and regulations provide organizations with strong incentives to protect this information.

The threat of litigation arises whenever the (real or perceived) failure of an organization's information security system affects another party. In addition to damage caused by the release of confidential information (e.g., medical records or financial records), damage may also include impairment of another party's computer system (including data, hardware, and software) from passing on a computer virus, libelous statements about another party being made on the organization's (tampered with) Web site, or participating (voluntarily or involuntarily) in a denial-of-service attack that shuts down the Web site of a third party. Investing in information security to comply with current industry practices and legal and regulatory requirements, along with careful documentation of the analysis underlying cybersecurity investment decisions, provides organizations with some degree of protection.

Legal and regulatory requirements vary across industries and tend to be more stringent in some industries than in others. Among those industries with especially strict requirements are the healthcare and financial sectors. Prominent examples of the types of requirements in these industries are the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[9] and the Gramm-Leach-Bliley Act of 1999 (GLBA),[10] which are concerned with protecting

[9] For the full text of this legislation, see Health Insurance Portability and Accountability Act (1996).

[10] For the full text of this legislation, see Gramm-Leach-Bliley Act (1999).