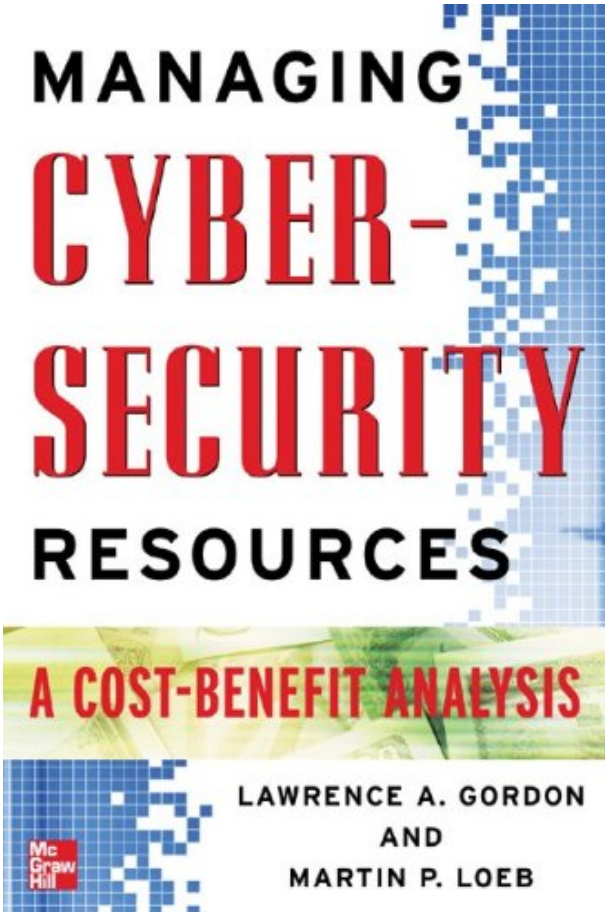
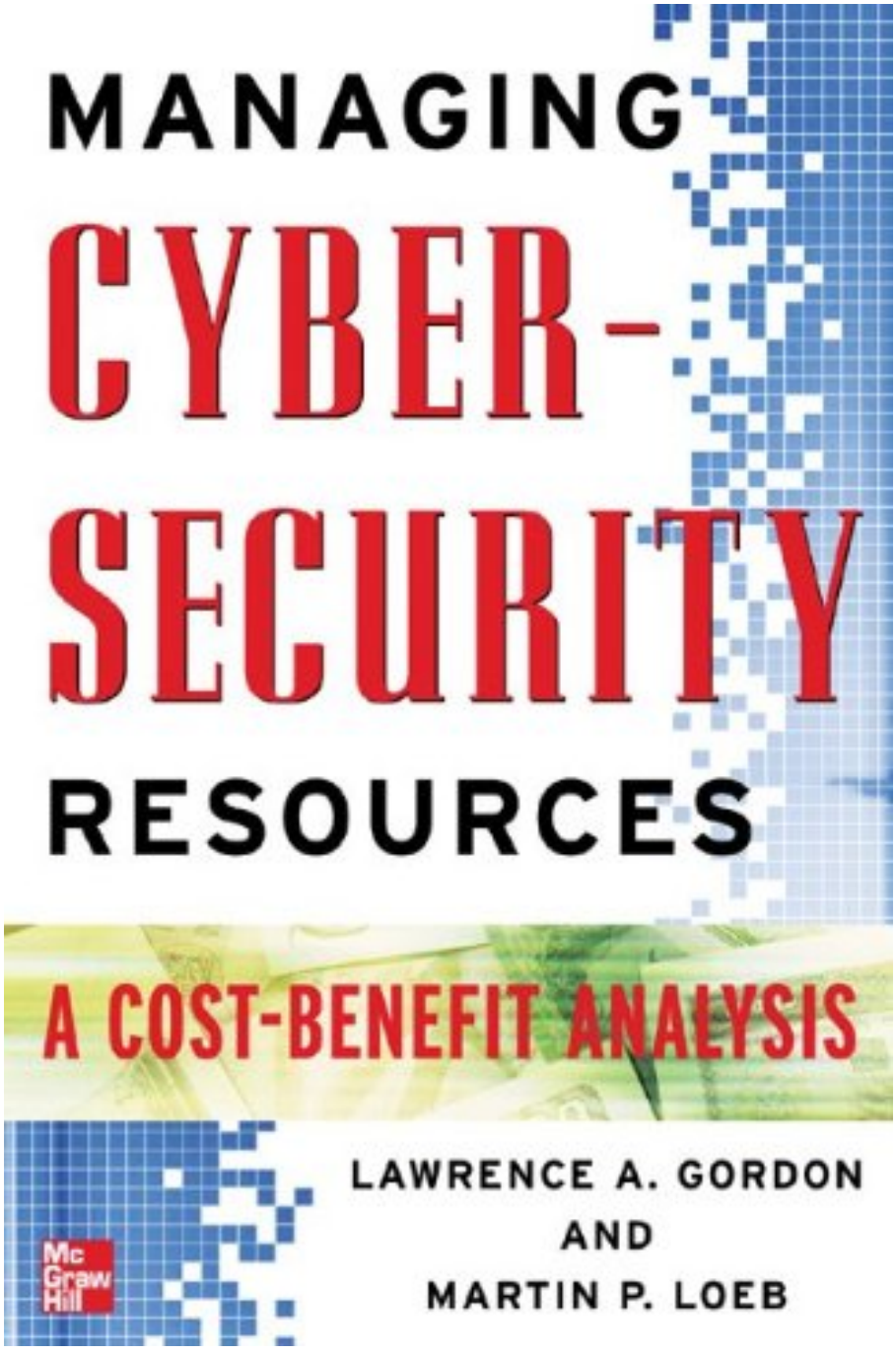
MANAGING CYBERSECURITY RESOURCES: A COST-BENEFIT ANALYSIS (THE MCGRAW-HILL HOMELAND SECURITY SERIES) BY LAWRENCE GORDON, MARTIN LOEB




Free Download



MANAGING CYBERSECURITY RESOURCES: A COST-BENEFIT ANALYSIS (THE MCGRAW-HILL HOMELAND SECURITY SERIES) BY LAWRENCE GORDON, MARTIN LOEB PDF

What do you do to start reviewing **Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb** Searching the publication that you love to read first or discover an interesting book Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb that will make you would like to review? Everyone has distinction with their reason of checking out a book Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb Actuary, reviewing habit must be from earlier. Many people could be love to review, yet not a publication. It's not mistake. An individual will certainly be bored to open the thick book with tiny words to check out. In more, this is the genuine condition. So do take place most likely with this Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb

MANAGING CYBERSECURITY RESOURCES: A COST-BENEFIT ANALYSIS (THE MCGRAW-HILL HOMELAND SECURITY SERIES) BY LAWRENCE GORDON, MARTIN LOEB PDF

Is **Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb** publication your preferred reading? Is fictions? Exactly how's regarding record? Or is the very best seller novel your choice to fulfil your extra time? And even the politic or religious publications are you searching for now? Here we go we offer Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb book collections that you require. Great deals of varieties of books from several industries are provided. From fictions to scientific research and also religious can be searched and also found out here. You may not worry not to locate your referred publication to check out. This Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb is among them.

The way to get this publication *Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb* is very simple. You may not go for some places and spend the moment to only find the book Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb As a matter of fact, you may not always obtain guide as you agree. But here, only by search and locate Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb, you can get the lists of the books that you really expect. In some cases, there are lots of publications that are revealed. Those books naturally will certainly astonish you as this Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb compilation.

Are you interested in mostly publications Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb If you are still perplexed on which one of the book Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb that must be purchased, it is your time to not this website to look for. Today, you will certainly need this Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb as the most referred book and also a lot of needed book as resources, in other time, you can appreciate for a few other publications. It will certainly depend upon your prepared demands. But, we always recommend that publications Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb can be a fantastic problem for your life.

MANAGING CYBERSECURITY RESOURCES: A COST-BENEFIT ANALYSIS (THE MCGRAW-HILL HOMELAND SECURITY SERIES) BY LAWRENCE GORDON, MARTIN LOEB PDF

Breaches in cybersecurity are on the rise. Between 1998 and 2003, reported cybersecurity incidents increased over thirty-fold. Well-publicized information security breaches have made cybersecurity a critical and timely topic for the general public, as well as for corporations, not-for-profit organizations and the government. As a result, organizations need to be able to make the business case for spending the right amount on cybersecurity. They also need to know how to efficiently allocate these funds to specific cybersecurity activities. Managing Cybersecurity Resources is the first book to specifically focus on providing a framework for understanding how to use economic and financial management tools in helping to address these important issues. The McGraw-Hill Homeland Security Series draws on frontline government, military, and business experts to detail what individuals and businesses can and must do to understand and move forward in this challenging new environment. Books in this timely and noteworthy series will cover everything from the balance between freedom and safety to strategies for protection of intellectual, business, and personal property to structures and goals of terrorist groups including Al-Qaeda.

- Sales Rank: #1643530 in Books
- Published on: 2005-09-28
- Original language: English
- Number of items: 1
- Dimensions: 9.10" h x .88" w x 6.00" l, 1.11 pounds
- Binding: Hardcover
- 224 pages

Most helpful customer reviews

8 of 9 people found the following review helpful.
An excellent book with only one major flaw
By Richard Bejtlich
Managing Cybersecurity Resources (MCR) is an excellent book. I devoured it in one sitting on a weather-extended flight from Washington-Dulles to Boston. MCR teaches security professionals how to think properly about making security resource allocation decisions by properly defining terms, concepts, and models. The only problem I have with MCR is the reason I subtracted one star: its recommended strategy, cost-benefit analysis, relies upon estimated probabilities of loss and cost savings that are unavailable to practically every security manager. Without these figures, constructing cost-benefit equations as recommended by MCR is impossible in practice. Nevertheless, I still strongly recommend reading this unique and powerful book.

My favorite aspect of MCR is its explanation of economics and finance terms to the security audience. I felt like applauding when I read on p 47 "[M]any managers... are merely calling the IRR an ROI or ROSI (return

on security investment). Given that the concepts of "return on investment" and "internal rate of return" are well established in the accounting, finance, and economics literature, as well as among nearly all senior financial managers (e.g., CFOs), security managers should be careful how they use these terms. Indeed, misusing these terms can only lead to problems for the security manager." (See p 45 for a comparison of ROI, IRR, and NPV.)

In a similar fashion, MCR explains what a "return" is for security on p 21: "The benefits associated with cybersecurity activities are derived from the cost savings (often called cost avoidance) that result from preventing cybersecurity breaches. These benefits are difficult, and often impossible, to predict with any degree of accuracy. Moreover, since the actual benefits are conceptually the cost savings associated with potential security breaches that did not occur, it is not possible to measure these benefits precisely after the security investments are made."

What of "investment"? Pp 28-30 say: "[O]rganizations tend to treat the bulk of their cybersecurity expenditures as operating costs and charge them to the period in which they are incurred," unlike capital investments, which "represent assets of an organization that should appear on the organization's balance sheet." The authors recommend us to "view all costs related to cybersecurity activities... as capital investments with varying time horizons."

So what is a cost? P 5 says "The cost of information security is essentially a negative network externality associated with the Internet... [It] arises when malevolent individuals and organizations [which the authors properly label "threats" on p 12] 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 cost of actions... designed to prevent such breaches."

P 30 wisely states "[N]o amount of security can guarantee that breaches will not occur... The goal of the organization should be to implement security procedures up to the point where the benefits minus the costs are at a maximum." The footnote on p 31 continues with "An alternative way to view this discussion is to think of the goal as one of trying to minimize the sum of the costs associated with cybersecurity activities and the costs associated with breaches... the optimal level of cybersecurity for an organization would be the same under the cost minimization goal as it would be if the organization were to maximize the net benefits." I think most managers prefer to think in terms of cost minimization, which is a prevalent throughout IT.

Costs are dissected on pp 56-58: "The direct costs of cybersecurity breaches are those costs that can be clearly linked to specific breaches... the indirect costs of cybersecurity breaches cannot be linked... Explicit costs of cybersecurity breaches are those costs of breaches that can be measured in an unambiguous manner... implicit costs are opportunity costs (i.e., costs associated with lost opportunities), which cannot be measured without ambiguity... the benefits derived from spending funds on cybersecurity activities come largely from the cost savings derived by avoiding the implicit costs of breaches."

Page 63 explains why companies have "Chief Privacy Officers" and the like, even though preserving privacy is the confidentiality aspect of the CIA triad and could be a CISO responsibility: "The findings from our study show that, on average, information breaches that compromise confidentiality do have a significant negative impact on the stock market value of corporations experiencing breaches. Indeed, the average decline in the firm's stock market value... was approximately 5 percent."

So far so good, right? The major flaw with MCR arrives in ch 4, on p 68: "The variables affecting potential cost savings include (1) the potential losses associated with information security breaches, (2) the probability that a particular breach will occur, and (3) the productivity associated with specific investments, which

translates into a reduction in the probability of potential losses." This is true -- but this is the key problem: devising even rough estimates of 1, 2, and 3 is nearly impossible in practice. The authors' examples (see figure 4-2 for one) assume these factors can be determined (like $10 mil total potential loss without countermeasures, 75% probability of loss with no countermeasures / 50% with $650,000 of countermeasures, and so on). When I saw these contrived examples I wondered "what is the origin of these figures?" The fact of the matter is that they are all guesswork, which means the calculator can say anything the analyst wishes to produce.

In some sense we are back to square one, although much better educated in economics. (Note that Andy Jaquith's book Security Metrics also observes how calculating these figures is nearly impossible in real life.)

Because MCR is so right in all of its other discussions, the book deserves 4 stars. A proper acceptance of the difficulty or impossibility of determining 1, 2, and 3 might have resulted in 5 stars. Perhaps a second edition will address these concerns?

PS: I would be remiss to not quote the authors' exceptional insights into the problems with security auditing. P 132 says "[T]he checklist approach tends to shift attention away from the cost-benefit aspects of such security. That is, the checklist approach usually assumes that conducting a particular procedure is inherently worth doing." P 137 hits the nail on the head: "[F]or some firms, it is quite possible that the costs of cybersecurity auditing will exceed the benefits. If this were to occur, then cybersecurity auditing would in effect decrease the firm's value." Amen.

5 of 5 people found the following review helpful.
An excellent economic analysis of cybersecurity investments
By Krishnamurthy Surysekar
This book is very timely and extremely useful as a tool for key decision-makers in organizations - Chief Technology Offiers, Information System Managers, and general managers, including CEOs, as well as academics. How do you allocate scarce resources to increasing cybersecurity, in the context of other competing claims ? Professors Gordon and Loeb provide a solid economic framework to do this. They bring their decades of experience researching and teaching about a cost-benefit approach to managerial decisions to the table, in the context of cybersecurity investments.

What I like about the book is its appeal to practitioners and academics alike. There is a nice section on developing a business case for cybersecurity investments. Empirical evidence to support their arguments are provided throughout the book. Complex ideas like real options and cybersecurity investments are nicely explained with simple and insightful examples.

Overall, whether you are a manager making or evaluating the case for cybersecurity investments, or teaching in this area, this book is a must-read.

9 of 9 people found the following review helpful.
Managing Cybersecurity Resources: A Cost-Benefit Analysis
By Joseph Aharony
Managing Cybersecurity Resources: A Cost-Benefit Analysis is excellent! Information security practitioners will appreciate the insightful economic analysis on how to determine the right amount to spend on cybersecurity projects and how to prepare a business case to justify such projects. I especially liked the chapter on risk that included perspectives and analysis not found in any other information security books. The book discusses many topics (for example, economics of cybersecurity and its role in national security) in a manner that novice and expert alike will find appealing. Its clear that the authors, chaired professors from a top business school and pioneers in cybersecurity economics, have a strong understanding of the security

environment along with great technical skills. Of more importance, is their intuitive understanding of problems in the cybersecurity trenches. Policy makers, CISOs, CFOs, and managers at all levels, should find enormous value in this book. While at times I wish the authors would not have condensed their discussion, the good news is that they have left some important issues for a follow-up book. I am recommending this book to co-workers and friends.

See all 4 customer reviews...

MANAGING CYBERSECURITY RESOURCES: A COST-BENEFIT ANALYSIS (THE MCGRAW-HILL HOMELAND SECURITY SERIES) BY LAWRENCE GORDON, MARTIN LOEB PDF

Even we discuss guides **Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb**; you may not find the printed books here. A lot of collections are provided in soft documents. It will precisely offer you a lot more perks. Why? The initial is that you may not need to lug guide everywhere by fulfilling the bag with this Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb It is for the book remains in soft documents, so you can save it in gizmo. Then, you can open up the gizmo all over as well as check out the book appropriately. Those are some few benefits that can be got. So, take all advantages of getting this soft documents publication Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb in this site by downloading in link provided.

What do you do to start reviewing **Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb** Searching the publication that you love to read first or discover an interesting book Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb that will make you would like to review? Everyone has distinction with their reason of checking out a book Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb Actuary, reviewing habit must be from earlier. Many people could be love to review, yet not a publication. It's not mistake. An individual will certainly be bored to open the thick book with tiny words to check out. In more, this is the genuine condition. So do take place most likely with this Managing Cybersecurity Resources: A Cost-Benefit Analysis (The Mcgraw-Hill Homeland Security Series) By Lawrence Gordon, Martin Loeb