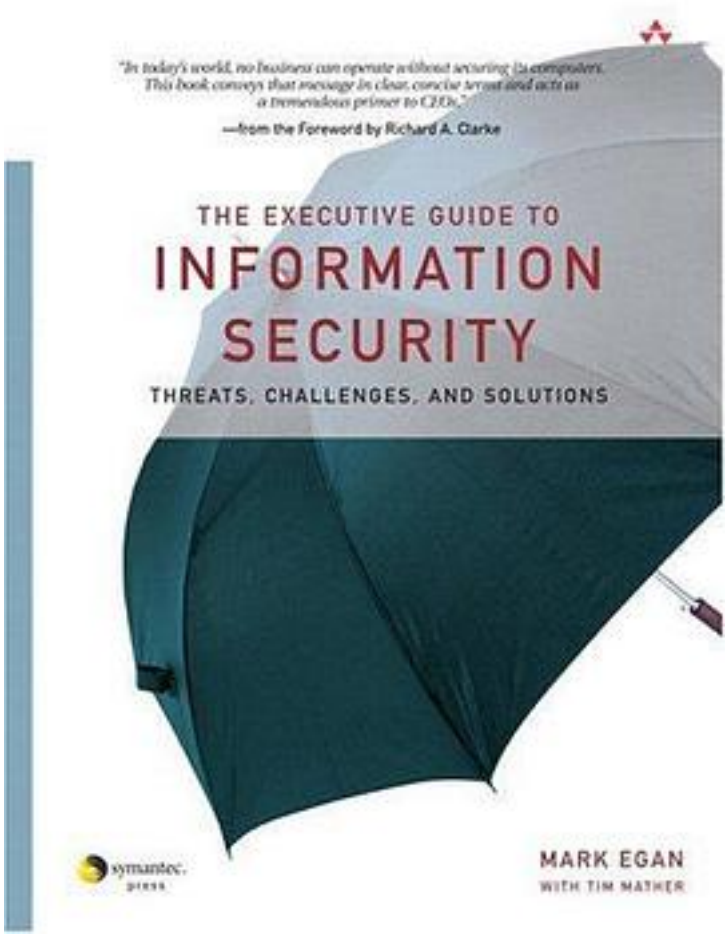
The Executive Guide to Information Security



The Executive Guide to Information Security_下载链接1_

著者:Mark Egan

出版者:Addison-Wesley Professional

出版时间:2004-11-30

装帧:Paperback

isbn:9780321304513

Preface Preface Who Is This Book For This book is devoted to executives who could benefit from a crash course on information security. We know that you are quite busy, so you need practical recommendations that you can implement quickly. In this book,

information security concepts are explained in nontechnical terms to enable executives from any discipline to quickly understand key principles and how to apply them to their business. This book provides a pragmatic approach to evaluating security at your company and putting together an information security program. Key elements of the program include staffing this function at your company, putting the necessary internal processes in place, and implementing the appropriate technology. Business executives will find this book a good primer for understanding the key existing and future security issues and for taking the necessary actions to ensure the protection of their enterprise s information assets. Information Security Background Information security is no longer an issue that is the responsibility of lower-level staff in the information technology (IT) department. Companies are now conducting a significant portion of their business electronically and need to be confident that their systems are safe and secure. This issue has now been escalated to the Board of Director level, and companies need to take information security seriously. The passage of the Sarbanes-Oxley Act has caused boards and especially audit committees to get much more involved in monitoring the performance and security of key information systems. This act requires companies to make new disclosures about internal controls and includes significant penalties and possible prison terms for executives of companies that are not in compliance. When I started with Symantec in 1999, information security was slowly becoming a major issue that executives had to address. More business was being conducted on the Internet, and system outages gained much more attention from the media. Many companies did not have formal information security programs, and security issues were addressed in an "ad hoc" fashion. Technology solutions at that time consisted mainly of firewalls and anti-virus software that operated independently. One of my challenges with my new position was to quickly gain an understanding of information security because Symantec had shifted its focus to address this market. Most of the literature that was available was very technical and did not provide a good overview for executives of how to put an effective information security program in place. Considering that I had spent the prior 25 years working in information technology, this would have been even more difficult for executives from other disciplines to understand. The industry has changed considerably over the past few years, and a simple virus that was a minor annoyance in the past has shifted to major threats such as Code Red that have caused major disruptions to businesses. Unfortunately, the future does not hold much promise for things to improve, and businesses will need to devote much more attention to this area. The objective of this book is to provide a shortcut for executives to learn more about information security and how it will affect their business in the future. An overview of information security concepts is provided so that executives can be better prepared to evaluate how their company is addressing information security. Pragmatic approaches are provided to assist companies in improving their information security programs. How This Book Is Organized This book focuses on three key themes: people, processes, and technology. These are the key elements of an effective information security program, and it is important to balance these components of the program. Considerable attention has been given to technology in the media and information security literature. However, this is just one element of an effective overall program. The best technology is not going to help if you do not have good staff and processes in place. This book is organized according to the steps you would follow to develop an information security program for your company. Chapter 1, "The Information Security Challenge," provides an overview of information security challenges and why executives should pay attention to the potential risks that these challenges pose to their business. A historical review of the Internet and information security incidents is also covered, and the chapter offers some insight into the power and vulnerability of conducting business electronically. Chapter 2, "Information Security Overview," provides an introduction to information security and the key elements of an effective program. The Security

Evaluation Framework is introduced in Chapter 3, "Developing Your Information Security Program," and can be used to evaluate your information security program and develop a roadmap to improve your program. The overall methodology is reviewed, along with the critical areas to ensure success. The next three chapters are devoted to evaluating the people, process, and technology components of your information security program and developing an improvement plan. Chapter 7, "Information Security Roadmap," pulls all this analysis together and describes how to develop your roadmap to an improved information security program that is appropriate for your company. Future trends for information security are reviewed in Chapter 8, "View into the Future," which offers some insight into emerging threats and industry solutions to address these threats. This field is changing rapidly, and it is important to always keep up to date on the latest events. The final chapter lists the 10 essential components to an effective information security program and offers a good summary for anyone who wants to quickly identify areas for improvement. Additional sources of information and references are included in the appendixes. One final point is that this book is written from a vendor-neutral perspective; it does not contain references to commercially available security products and services. The focus is on industry best practices for information security. Due to the rapid changes in this industry, it is difficult to predict which companies will lead as the market evolves. The concepts outlined in this book can serve as a guide to choosing the appropriate products and services to support your program today and in the future. /> class="navigation">

作者介绍:

目录:

The Executive Guide to Information Security_下载链接1_

标签

评论

The Executive Guide to Information Security_下载链接1_

书评

The Executive Guide to Information Security_下载链接1_