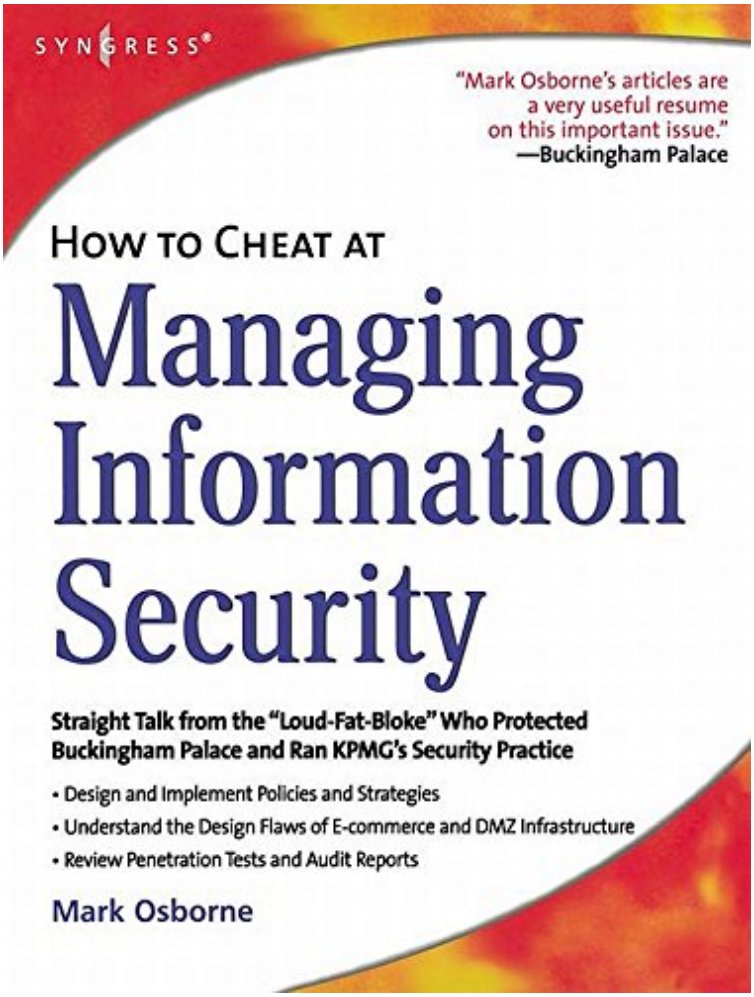
How to Cheat at Managing Information Security

Mark Osborne
*ebooks | Download PDF | *ePub | DOC | audiobook*



#2870224 in eBooks 2006-08-22 2006-08-22File Name: B00M3Z1D2O | File size: 76.Mb

Mark Osborne : How to Cheat at Managing Information Security before purchasing it in order to gage whether or not it would be worth my time, and all praised How to Cheat at Managing Information Security:

5 of 5 people found the following review helpful. The adventures of an information security professional and his efforts to secure corporate networksBy Ben RothkeMark Osborne doesn't like auditors. In fact, after reading this book, one gets the feeling he despises them. Perhaps he should have titled this book 'How I learned to stop worrying and hate auditors'. Of course, that is not the main theme of How to Cheat at Managing Information Security, but Osborne never hides his feeling about auditors, which is not necessarily a bad thing. In fact, the auditor jokes start in the preface, and continue throughout the book.The subtitle of the book is 'Straight talk from the loud-fat-bloke who protected Buckingham Palace and ran KPMG's security practice'. Essentially, the book is Osborne's reminiscence of his years in information security; including the good, the bad, and more often then not, the ugly.The book is written for someone looking to develop an information security program, or strengthen an existing program, to ensure that all of the critical technology areas are covered.The thirteen chapters of the book cover the main topics that an information security

manager needs to know to do their job. The author candidly notes that this book is not the most comprehensive security book ever written, but contains most of the things a security manager needs to get their job done. The author also observes that information security is different from other disciplines in that there are many good books about disconnected subjects. The challenge is getting the breadth of knowledge across these many areas, which is quite difficult. The challenge of information security is to effectively operate across these many areas.Chapters 1 and 2 deal with the information security organization as a whole, and the need for information security policy. Chapter 1 details the various areas where a security group should be placed, and describes the pros and cons of each scenario. As one of the scenarios which place information security below the head of audit, Osborne notes that 'if you have any sort of life, you don't want to spend it with the auditors, I promise you'.Wherever the security group is placed in an organization, its ultimate success or failure is likely to be determined by its level of autonomy and independence. Unfortunately, in far too many organizations, information security is not given that liberty. It is often placed in a subservient role to groups with opposing interests. Any security group or security manager placed in such a situation should likely start working on their resume.The scenario is described in 'Practical Unix and Internet Security' where author Professor Gene Spafford spells out Spaf's first principle of security administration. This principle states that 'if you have responsibility for security but have no authority to set rules or punish violators, your own role in the organization is to take the blame when something big goes wrong'. Spaf's principle is a cruel reality faced by many of those responsible for information security.Between those chapters and a few more auditor jokes, Osborne makes the blatently obvious observation that wherever possible, one should eradicate single points of failure. As a corollary to this, Osborne notes that while trying to eliminate these failure points, companies will often build redundant systems. Part of their admiration for these redundant systems is the hope that this will simultaneously reduce performance bottlenecks. But these companies do not realize that the routers, firewalls and switches are not the bottleneck, rather it is the software application which is the bottleneck.Osborne plays the role of contrarian in chapter 8 when he asks why we need firewalls. He notes that if every database maker, operating system programmer and CRM/ERM vendor put as much effort into security as the firewall vendors do, then there would be no need for firewalls. Furthermore, if each system administrator worked as hard on security as the typical firewall administrator did, and devoted as much time to hardening their servers and laptops as they did; then centralized firewalls would likely not be needed. Given that the firewall-free reality is not happening any time soon, chapter 8 provides a lot of good information on everything you need to know about firewalls.Chapter 9 is about one of the most maligned security tools, the IDS. After providing an anecdote about a network manager who did not understand the fundamentals of how DHCP operates, and how he used Snort to debug the problem; Osborne provides a meaningful piece of security wisdom when he notes that IDS can help any network or security person understand network traffic. These devices can even give you information on new attacks and how they can be mitigated. But for an IDS (or any security hardware or software device for that matter) to be truly useful, a security professional needs to understand their IT infrastructure, the mechanics of networks and applications and the risks involved. Those who don't understand those three things will only be able to use these security technologies with minimal benefit.Overall, How to Cheat at Managing Information Security, is an informative and often entertaining introduction to information security. For those that want to get a good overview of the core elements of information security, or strengthen their existing knowledge base, they will find this book to be an informative and valuable read."13 of 15 people found the following review helpful. Security is a lifestyleBy ueberhundSecurity isn't just something you "turn on". Security is a mindset, a set of systems and practices that affect all aspects of your work environment. And implementing security practices--especially in an organization devoid of such--is a daunting task. I found this to be an excellent book in that the author obviously understands security. He's dedicated his life keeping privileged information safe. More importantly, this book is laid out in such a way that it will lead the uninitiated, newly appointed security expert at any organization through the process of implementing a security framework.Firewalls, Intrusion Detection Systems, and the like are only as good as the policies that govern them. The first step in implementing security is to define an information security policy. The author leads the reader through identifying business risks and creating an action plan to mitigate those risks.In addition to the expected "what does a firewall do, and how should you use it" type of information, the author does an excellent job cutting to the chase on a wide variety of security issues. He provides examples of how find the right people to implement your security framework, what types of systems might be required in your environment, and how to perform periodic penetration testing, to see if your security framework keeps the bad guys out.I really see this book being of great benefit to the newly appointed security expert, who is perhaps a bit overwhelmed with his/her new responsibilities. This book is an easy read, very interesting, and very useful for the individual responsible for all aspects of a company's security infrastructure.4 of 8 people found the following review helpful. Works For Me!By A. ReviewerThis book fits the bill for me!!. And it is enjoyableI have a number of other handbook style books - one that cost nearly six times more but was really a collection of articles written by a dozen different people (some with obviously conflicting views) bound under the same cover.What I liked:This book simply sets out the things I need to know about Organisations, Strategies and Audits then progresses into firewall design and security testing. And it is so funny - the cover is right this man does make security light going.What could be better:The guy is obviously technical so at the

end some of it is a bit hard going - just I had to skip bits. But each chapter is laid out so that the chapter gets more complex at the end so this wasn't a problem.I would have liked more on Virus technology and Wireless security - especially as after work on Google, I understand that the fat-bloke was a leading researcher in wireless securityOverall conclusion: Great.

This is the only book that covers all the topics that any budding security manager needs to know! This book is written for managers responsible for IT/Security departments from mall office environments up to enterprise networks. These individuals do not need to know about every last bit and byte, but they need to have a solid understanding of all major, IT security issues to effectively manage their departments. This book is designed to cover both the basic concepts of security, non ndash; technical principle and practices of security and provides basic information about the technical details of many of the products - real products, not just theory. Written by a well known Chief Information Security Officer, this book gives the information security manager all the working knowledge needed to: bull; Design the organization chart of his new security organization bull; Design and implement policies and strategies bull; Navigate his way through jargon filled meetings bull; Understand the design flaws of his E-commerce and DMZ infrastructure* A clearly defined guide to designing the organization chart of a new security organization and how to implement policies and strategies* Navigate through jargon filled meetings with this handy aid* Provides information on understanding the design flaws of E-commerce and DMZ infrastructure