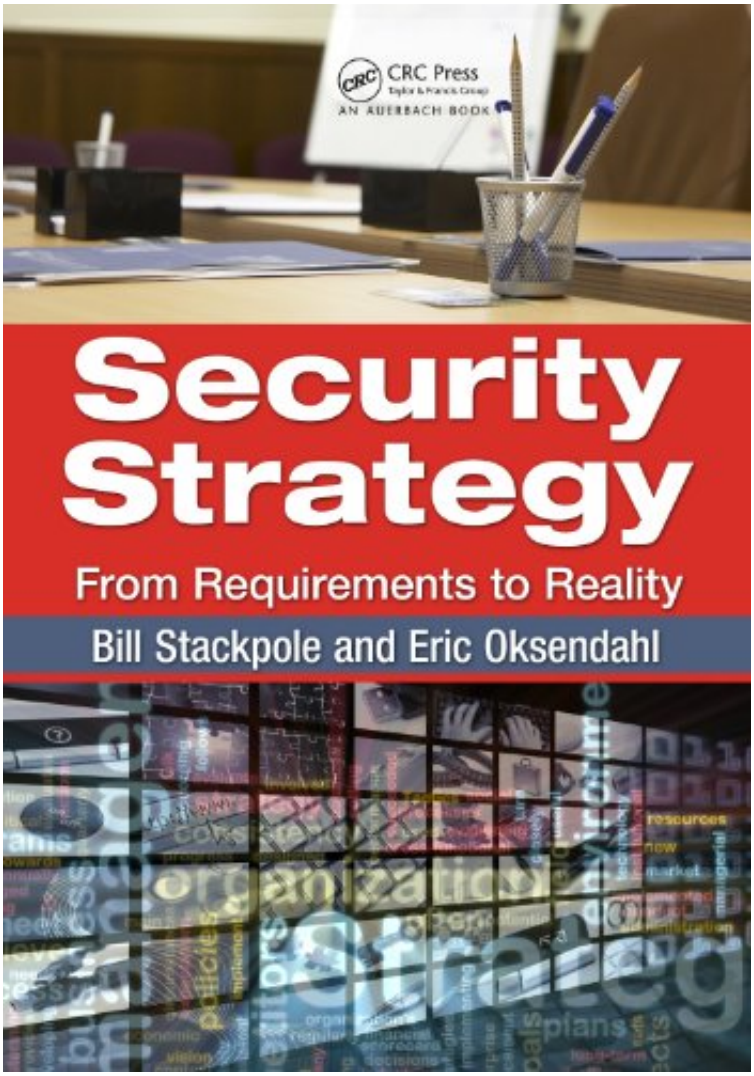
# Security Strategy: From Requirements to Reality

*Bill Stackpole, Eric Oksendahl*
*DOC | *audiobook | ebooks | Download PDF | ePub*






#1250410 in eBooks 2010-10-13 2010-10-13File Name: B00918NKGI | File size: 57.Mb

**Bill Stackpole, Eric Oksendahl : Security Strategy: From Requirements to Reality** before purchasing it in order to gage whether or not it would be worth my time, and all praised Security Strategy: From Requirements to Reality:

4 of 4 people found the following review helpful. One of the best information security books of the last few yearsBy Ben RothkeSecurity Engineering: A Guide to Building Dependable Distributed Systems by Ross Anderson is arguably the best information security book ever written. Anderson's premise is that security technology needs to take a structured engineering approach to systems design, with detailed requirements and specification from start-up to development and implementation; just as those designing buildings and bridges do. Without a deeply embedded structured approach to security systems design, Anderson argued that we find ourselves in the situation we are in today, with applications and operating systems full of bugs, vulnerabilities and other serious security flaws.As good as

Security Engineering is, it was not written to be a detailed information security design guide. That vacuum has been filled by an incredibly important and valuable new book Security Strategy: From Requirements to Reality.Security Strategy is one of the first books that shows how to perform a comprehensive information security assessment and design, from section, development and deployment of a security strategy best suited to a specific organization.The books main focus is on the planning, requirements and execution need to ensure formal and comprehensive information security elements are built into systems, applications and processes.Authors Bill Stackpole and Eric Oksendahl each have over 25 years in the industry and the book reflects their vast expertise. Oksendahl spent time at Boeing, one of the most security aware organizations, with Stackpole spending a decade at Microsoft. While Microsoft is chided for creating more insecurity than security, it is worth noting that no organization in the world has spent more on training its staff and developers on security than Microsoft.The books 300 densely written pages are composed of 14 chapters divided into 2 sections. Section one (chapters 1-6) is about strategy, with section two (chapters 7-14) around tactics.Complete with checklists of the physical security requirements that organizations should consider when evaluating or designing facilities, the book provides the insight needed to enable an organization to achieve the operational efficiencies, cost reductions, and brand enhancements that are possible when an effective security strategy is put into action.Chapters 1-3 take a high-level overview on how to approach strategy, with its many details. The authors note that strategy is a long-term plan of action designed to achieve a goal that includes what work will be done and by whom. This is not a trivial task, as many organizations simply roll-out a new technology, without defining what its goals are, and who exactly will manage and support this new technology.Chapter 4 is where the hard work begins, as this chapter details the issues around strategic planning. Noting that strategic security planning is hard work and takes time; many organizations attempt to take an assumed easier path, that of bypassing security details and specifications. That is precisely why information security is in such a sorry state in many firms. These firms would rather buy a security appliance and place it in their data center and hope it works; rather than defining the details and specifications of what the appropriate appliance is in the first place.Part 2 commences on the topic of tactics, and defines them as procedures or sets of actions used to achieve a specific objective. What this chapter does well, as does the entire book, is that it compels the reader to focus on specifics and objectives.Chapter 9 gets into the importance of observation, in knowing what is going on within the network. The book notes that observation is both a deterrent and a detector. The chapter goes into detail about how observation works both in the physical world and its corollary use in the network side. The chapter breaks down the various functions needed to ensure that observation is done correctly; as opposed to the common method of simply rolling out an IDS and hoping that it somehow works.Chapter 11 details the SDL (security development lifecycle). As the chapter notes, an effective SDL can improve application security via the use of a set of development practices designed to reduce or eliminate exploitable vulnerabilities. The issue though is that far too few organizations realize the need for a SDL, let alone take the time to design and deploy it.Chapter 14 ends on the topic of security awareness training. While the notion of security awareness for many firms is an annual 10-slide PowerPoint; the authors take a pragmatic approach and detail the various parts of what makes for an effective awareness program.Security Strategy: From Requirements to Reality is an incredibly valuable book that advances the state of information security. For organizations that are looking to get serious about information security, and those that want to go from good to great, the book is an invaluable guide that lays the groundwork on how to develop a first-rate information security infrastructure.Taking a look at its table of contents shows the many fine points in which the book goes into each particular point, showing how it can be properly designed and deployed for effective security controls.My only peeve with the book is that it lacked a CD-ROM or web site in which to download the many tables and matrices the book is built on. It is hoped that future editions will have them available.Security Strategy: From Requirements to Reality is one of the best information security books of the last few years. Those who are serious about information security will ensure this is on their reading list, and that of everyone in their organization tasked with information security.0 of 8 people found the following review helpful. Do NOT buy kindle edition!By Kevin DavidsonI would love to review the book, but the Kindle edition is not worth it!1. It cannot be delivered to any Kindle except the Fire or Fire HD2. There is no zoom or font choices. It is like they OCR'd the pages. The only way to read this book is with a magnifying glass or manually zoom sections of the page. Take your smallest font for a normal book, and cut it in half. That is what the entire book is, and the normal font size options are not available.Might be a great book-authors are well-respected in the industry.

Addressing the diminished understanding of the value of security on the executive side and a lack of good business processes on the security side, Security Strategy: From Requirements to Reality explains how to select, develop, and deploy the security strategy best suited to your organization. It clarifies the purpose and place of strategy in an information security program and arms security managers and practitioners with a set of security tactics to support the implementation of strategic planning initiatives, goals, and objectives. The book focuses on security strategy planning and execution to provide a clear and comprehensive look at the structures and tools needed to build a security program that enables and enhances business processes. Divided into two parts, the first part considers business strategy and the second part details specific tactics. The information in both sections will help security practitioners and mangers

develop a viable synergy that will allow security to take its place as a valued partner and contributor to the success and profitability of the enterprise. Confusing strategies and tactics all too often keep organizations from properly implementing an effective information protection strategy. This versatile reference presents information in a way that makes it accessible and applicable to organizations of all sizes. Complete with checklists of the physical security requirements that organizations should consider when evaluating or designing facilities, it provides the tools and understanding to enable your company to achieve the operational efficiencies, cost reductions, and brand enhancements that are possible when an effective security strategy is put into action.

This book focuses on the process, objectives, and controls of security strategy. It consists of two sections: Strategy (6 chapters) and Tactics (8 chapters). The sections include strategy how-torsquo;s and security tactics, which support the realization of security. The strategy portion is aimed at executives, whereas the tactics portion is geared toward security professionals. hellip; The authorsboth security veteransshare many personal anecdotes. They use relevant quotes and concisely illustrate their points. The book addresses security quality attributes promoted by the Architecture Tradeoff Analysis Method (ATAM) and used in the Sherwood Applied Business Security Architecture (SABSA) framework hellip; .A. Marlen, s.com About the AuthorWilliam ldquo;Billrdquo; Stackpole, CISSP/ISSAP, CISM, former Principal Security Architect for Microsoft Online Services, has more than 25 years of IT experience in security and project management. In his past position, Bill provided thought leadership and guidance for Microsoftrsquo;s Secure Online Services Delivery Architecture. Before joining Microsoft, Bill was a principal consultant for Predictive System, an international network consultancy where he was the architect and promoted the application security business. Bill holds a B.S. degree in Management Information Systems, a CISSP with an Architecture Professional endorsement. He is co-author of Software Deployment,Updating, and Patching (Auerbach, 2007) and a contributing editor to Auerbachrsquo;s Handbook on Information Security Management (Krause and Tipton). Bill is a former chair for the CISSP Test Development Committee and a current member of the (ISC)2 Common Body of Knowledge committees for the CISSP and ISSAP certifications. Eric Oksendahl, former Security Strategist for Boeing, has more than 25 years of experience as a business management consultant, senior facilitator, teacher, and program manager. At Boeing, Eric facilitated strategy development and implementation for the Security and Fire Protection division, including physical and information security. He designed and coordinated the use of strategy development and initiative deployment to integrate security practices into key business processes (e.g., international sales campaigns). Prior to that, Eric was a program manager at the Boeing Leadership Center where he conducted leadership development courses around the world that included Boeing management, supplier management, and customer management. Eric holds a B.A. from Montana State University and an M.A. in Communications from the University of Washington.