Book Review

Security Risk Management: Building and Information Security Risk

Evan Wheeler
Elsevier Science
ISBN: 1597496154

Reviewed by: Pankaj Palvia, Ivy League Publishing, admin@ivylp.com

At a very general level, if you are the security manager for a company in-charge of protecting the company's information based assets from what goes into the trash to what has been put on the internet then this book is a good starting place. It will tell you how risk management has evolved over the years and how best to assess your company's risks. The book is designed to tell a risk manager how to do his job, what threats to look for from within and outside the company. It's well written and is not technical. If you're new to the field of information privacy and security then this book will be a good one to have as a handy reference on your desk.

Getting deeper into the book, I have to admit that the book is very well organized and one can get a very good sense of what is more to come by just quickly browsing through the table of contents. This should really help those who do not plan to read cover to cover and have an interest in just a particular area. Also, this book should really help the practitioner as it provides not only some useful techniques for use on a daily basis, but also the rationale behind these techniques. In my own experience, I have seen IT professionals fall into the trap of recommending techniques without providing a rationale. Furthermore, the author has generally done a good job of explaining how to break free from the "best practices" argument by explaining risk exposures in a lucid, simple to understand language. Among the techniques you will learn are:

- How to perform risk assessments for a totally new Information technology undertaking
- How to manage routine risk activities
- How to qualify existing risk level for presentation to decision-makers

I always enjoy books that include some real life examples. This book does a good job as case studies are included which a) provide practical insight into risk assessment tools and how cost benefits should be considered when looking at an investment in

security infrastructure, b) explore different phases of risk management lifecycle while focusing on processes and policies to mitigate risk, and c) present a walk through for designing and implementing a security management infrastructure.

Some of the case studies provide very useful and practical knowledge. One such study suggests that, whenever possible, serving static web pages to the public is much safer then dynamic pages. This is because the inherent complexity of the code in the later makes it more error-prone, and thus a good bait for a troublemaker.

Above knowledge should provide a big help to a CIO because it promotes building of a security risk management infrastructure based more on a customized approach rather then one based on the old "standard checklist" method. I believe this is the right approach in the present day world because technological advancements have made infrastructures more unique, thus making standardized approaches to building security infrastructure somewhat obsolete.

I recommend reading chapter 5 in greater detail by those that have difficulty in formulating risk and understanding its different components. This should help many beginning security professionals.

As one gets towards the end of the book, you will learn more advance topics and other approaches developed by security professionals.

In the end, this book will help you build a risk management program and show you the methods to implement thus keeping your information technology security structure state-of-the-art. Wheeler has done a good job in presenting a difficult topic in an easy to understand manner. The case studies are particularly helpful. The book is well written and will make a great reference tool for many information technology professionals and/or a IT security professionals.

Evan Wheeler, the author of the book, has spent six years as security consultant for the U.S.Department of Defense. His other professional career includes Director of Information Security at Omega, a Thomson Reuters Company

Pankaj Palvia is President and CEO of Ivy League Publishing and is also the founder of Tax & Accounting Advisors, a CPA firm located in Marietta, GA. Prior to the founding of Ivy League Publishing, Pankaj held mid-management level positions in corporate finance in such major companies as Digital Equipment Corporation, Coca Cola and Schreiber Foods.