Stepping Through the InfoSec Program

Posted by samzenpus on Mon Aug 11, 2008 12:59 PM
from the read-all-about-it dept.

Ben Rothke writes *"For those who want to stay current in information security, Stepping Through the InfoSec Program is a great book to read after The Pragmatic CSO: 12 Steps to Being a Security Master. While The Pragmatic CSO provides a first-rate overview of the higher-level steps to being a CSO and building an information security program, Stepping Through the InfoSec Program provides the low-level details and nitty-gritty elements on just how to do that."* Keep reading for the rest of Ben's review.

Stepping Through the InfoSec Program

author	J.L. Bayuk
pages	238
publisher	ISACA
rating	9
reviewer	Ben Rothke
ISBN	1604200308
summary	The low-down on how to build an information security program

Author Jennifer Bayuk spent over a decade at a large brokerage firm building their information security program. Her experience in managing and designing security there is manifest in the book and it is clear throughout the book that she is writing a deep pool of from real-world experience.

The first part of the book contains 3 sections and in just under 150 densely packed pages, the book walks you through the process in which to build an effective information security program. The book details 6 steps in which to facilitate this, namely: strategy, policy, awareness, implementation, monitoring and remediation.

The book starts out and begins to develop the context for an information security program. It astutely notes that an information security program exists only in the context of an organizational management structure. Anyone building an information security program for its own sake, removed from the organizational management structure will quickly find themselves devoid of a budget, and often shortly after that, out of a job.

The books attention to detail and specific definitions are superb. In the opening section, it defines the objectives, prerequisites, typical tasks and performance measures for over 10 different jobs within information security. It then creates a segregation of duties matrix for these jobs. Such detailed information is invaluable to anyone attempting to build a security program.

The main part of the book is in section 2 which steps through what an information security program is, how it is created, how it operates and what resources are required to maintain it. The beauty of the book is that the author understands that information security is not a monolithic undertaking. Rather it must be developed and customized according to the specific needs and requirements of the particular organization. These differences are made clear in the chapter when it details 9 unique information security reporting hierarchies; and deciding on the appropriate reporting hierarchy is not a trivial undertaking.

The book writes that successful information security program development, by definition, must align with organization goals. This alignment can only be achieved if the CISO has an open, two-way communication path to each manager with information security responsibilities. While this is a necessary and realistic goal, far too few CISO's have such communications paths at their disposal, and

even less have constituent ears that are receptive to such communications.

Section two provides an excellent overview of metrics and how they can be effectively used. In the last few years, metrics has been the rage in the security community. Individuals such as Pete Lindstrom and groups such as Security Metrics have been at the forefront of such efforts.

But the book notes that metrics for their own sake can also be taken too far. The book references a volume on metrics that has over 900 possible things to measure that would provide security metrics, including such silly metrics as "number of times, by fiscal year, that fines and jail sentences were imposed for altering, destroying, mutilating, concealing or falsifying financial records". Bayuk perceptively observes that any CISO who is measuring these types of concerns and analyzing them for feedback on how to improve their information security program should realistically look for a different job.

Section 3 concludes the main part of the book with a security program case study. The point of the case study is to show how an information security program evolves around changes in the organization it supports. The case study shows that all of the six steps on which the book is premised are indeed necessary.

The final 100 pages of the book detail various sample security policies, standards, procedures and guidelines. All of the policies, standards, procedures and guidelines are well-written and it would have been nice if these would have been available in electronic format.

The book notes that the information security professional has evolved from computer operator to chief information security officer; from controlling punched cards to negotiating strategic plans, defining policies, documenting processes, managing technology, measuring performance, controlling costs, supporting business recovery and demonstrating regulatory compliance. For those that want to make that transition, *Stepping Through the InfoSec Program* is a most valuable guide to get you there.

The book is written by an author who has significant amounts of real-world experience in a leading edge organization. That unique knowledge and experience is evident after reading the first few pages of the book. The book provides the reader with a comprehensive overview of how to build an effective information security organization.

One final note, don't judge a book by the cover. On the cover are three busy looking executives, all smiling and looking refreshed. The reality is that most people who have taken the time to build effective security programs often emerge from that battle exhausted and battle weary.

For anyone contemplation entering the information security field, or those in it already that need effective direction, *Stepping Through the InfoSec Program* should be on their required reading list.

Ben Rothke is the author of Computer Security: 20 Things Every Employee Should Know.