Enterprise Security for the Executive: Setting the Tone From the Top

By Jennifer L. Bayuk

Reviewed by C.W. Axelrod, Ph.D., CISM, CISSP, former business information security officer and chief privacy officer for U.S. Trust, Bank of America Private Wealth Management. Axelrod is currently a senior consultant with Delta Risk, which specializes in cybersecurity, risk management and business resiliency. He is a member of the Financial Services Sector Coordinating Council (FSSCC) Research and Development Committee and won ISACA’s 2009 Michael P. Cangemi Best Book/Best Article award. He was honored with the Information Security Executive (ISE) Luminary Leadership Award in 2007 and the ComputerWorld Premier 100 IT Leaders Award in 2003. Axelrod is the author of the book Outsourcing Information Security and coeditor of Enterprise Information Security and Privacy, both of which are available in the ISACA Bookstore.

Do you have something to say about this article? Visit the Journal pages of the ISACA web site (www.isaca.org/journal), find the article, and choose the Comments tab to share your thoughts.

Enterprise Security for the Executive: Setting the Tone From the Top, written by Jennifer Bayuk, appeared in November 2009, just two years after the author’s Stepping Through the InfoSec Program.

Bayuk’s books are typically compact, clearly written, well focused and easy to read, and they are frequently aimed at nontechnical corporate leadership and those information security professionals who see themselves as future managers. Both of these categories of readers will greatly benefit from reading Enterprise Security for the Executive: Setting the Tone From the Top.

The author worked as an information security professional in a major investment bank and securities firm for more than a decade. In preparing Enterprise Security for the Executive, she drew from her own vast experience and discussions with peers, most of whom were from similar large financial services firms. Therefore, the question arises whether a concentration in financial services such as the experiences depicted in the book can be considered truly representative of other sectors and of small to medium-sized businesses. The answer is “yes.”

Lessons from the banking and finance sectors are likely to be learned ahead of most other public and private sectors, and therefore, the experiences of those in this sector remain valuable to those in other sectors. Furthermore, since practically every human economic activity is dependent on the financial services industry, it behooves management in other sectors to understand the security strengths and weaknesses of this critical industry so that they are better equipped to deal with issues they may have with their financial institutions and within their own organizations.

The greatest value of Enterprise Security for the Executive: Setting the Tone From the Top is its description of information security practitioners’ experiences in dealing with C-level management and how those relationships should be handled. It is unusual to see so many actual experiences included in a single book and presented in such a way that readers can relate each experience to their own situations. Bayuk uses a creative tool in the form of security horror stories (SHSs) to illustrate and drive home the lessons of the text. The SHSs are not meant to impart fear, uncertainty and doubt on the part of the reader or the reader’s management, but to “illustrate the fact that, in the absence of systemic security management, disasters do happen.”

The book comprises introductory chapters on security threats and vulnerabilities; the security triad of confidentiality, integrity and availability; and secure products and services. Most security professionals should be well versed in these topics, but their managements likely will not match that expertise. On the other hand, the chapters on management structures for the security function and those dealing with legal and regulatory requirements will generally be more familiar to executives than to security engineers. As a result, the book has something for everyone, although it is clearly geared to senior management.

Readers should not skip the case study found in the appendix. While it is hoped that none of the readers are confronted with an environment such as the one depicted in the case, those who, at one time or another, have been tasked with establishing security programs from scratch can readily relate to the story.

As with some of the author’s prior works, Enterprise Security for the Executive provides valuable advice to the reader. However, the real value of the book is realized when read by senior managers, who are less likely to seek out such a book.

EDITOR’S NOTE

Enterprise Security for the Executive: Setting the Tone From the Top is available from the ISACA Bookstore. For information, see the ISACA Bookstore Supplement in this Journal, visit www.isaca.org/bookstore, e-mail bookstore@isaca.org or telephone +1.847.660.5650. Another resource is the ISACA Business Model for Information Security™ (BMIS™), posted at www.isaca.org/bmis.