

Stepping Through the InfoSec Program

By J. L. Bayuk, CISA, CISM

Review by C. Warren Axelrod, Ph.D., CISM, CISSP

This is the author's second "Stepping Through..." book. The first book, *Stepping Through the IS Audit*, was written to help both auditors and auditees through the intricacies of the information systems (IS) audit process. The second book, *Stepping Through the InfoSec Program*, tackles the broader and, in some ways, more challenging topic of establishing and running an information security program.

Although the second book is clearly directed at the information security manager, it could provide value to a number of constituencies. For one, IS auditors may find the book useful as a basis for determining what an ideal information security program should be. Business unit managers may benefit greatly from this book, particularly when dealing with the information security group, and less-technical readers will find the case study helpful to understand the key aspects of an information security program in operation.

While the covers of both books show three smiling professionals walking through a barrier of zeros and ones, Stargate style, most novices and many experienced security professionals likely envision the process of setting up and executing an information security program to be more like making their way cautiously through a minefield. Unfortunately, the latter description may indeed be more representative of the experience for many organizations as well. Consequently, the primary need is for no-nonsense, to-the-point guidance to establish and enforce an information security program; this is what the book provides so well.

If my experience is typical, the information security professional tasked with setting up an information security program starts out by writing policy. Once the security policy and standards have been dutifully copied from one of the many available sources, what should be done next? Without a realistic guide to the next steps, information security professionals may find themselves at a loss. This book is one such guide and can help professionals get over the hurdle.

Stepping Through the InfoSec Program consists of three sections: the context in which information security programs are developed, the components of the information security program itself and a case study in the form of a chatty but substantive dialog. Notably, the first part focuses on individuals, whereas the second and third parts focus on the program.

The first part provides a comprehensive background and a practical context, including:

- A description of the history leading up to today's information security programs
- An enumeration of the various job functions that relate to information and physical security

- Descriptions of the roles and responsibilities of those within the various functions
- A list of respected certifications in the field
- A discussion of metrics used to determine performance of the information security function

The second part presents the components of an information security program. It guides the reader through the following:

- Creation of the information security program
- Relating the information security program to information technology governance
- Ensuring accountability through roles and responsibilities
- Identification and location of resources to achieve objectives
- Determination that the program is meeting objectives

Because this second part is so full of information, issues and advice, it may require careful reading and rereading to internalize some of the most critical areas, but it is well worth the effort. Having conquered the concentrated information in the second part, the reader may find it to be somewhat of a relief to move into the third part, the case study.

The case study brings home the many lessons of the second part in a lighter, more readily digestible form. One gets the impression from the keenly crafted scenes that the author has actually lived through many of the scenarios described. This incorporation of dialog, which is a technique that was also used in the first book, is unusual for books of this type, but works well in reiterating the many concepts previously presented.

Following the three sections that comprise the body of the book are a number of useful appendices. Sample policy, standard, procedure and guideline documents are included. These serve not only as examples, but are also valid documents that could be used directly.

C. Warren Axelrod, Ph.D., CISM, CISSP

is the business information security officer and chief privacy officer for United States Trust Company, N.A. At US Trust, he identifies, assesses and mitigates privacy and security risks, and ensures that employees are familiar with privacy and security policy and procedures. Axelrod is involved in the financial industry and with cybersecurity and critical infrastructure issues at the national level.

Editor's Note:

Stepping Through the InfoSec Program 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.



Information Systems Control Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *Information Systems Control Journal* does not attest to the originality of authors' content.

© 2008 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by ISACA, for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org