Physical Security Systems Handbook

The Design and Implementation of Electronic Security Systems

MICHAEL KHAIRALLAH

B/H

PHYSICAL SECURITY SYSTEMS HANDBOOK

The Design and Implementation of Electronic Security Systems

PHYSICAL SECURITY SYSTEMS HANDBOOK

The Design and Implementation of Electronic Security Systems

Michael Khairallah, PSP

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO

Butterworth-Heinemann is an imprint of Elsevier

Elsevier Butterworth-Heinemann
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
Linacre House, Jordan Hill, Oxford OX2 8DP, UK

Library of Congress Cataloging-in-Publication Data
Application submitted.

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN 13: 978-0-7506-7850-6
ISBN 10: 0-7506-7850-X

For information on all Elsevier Butterworth–Heinemann publications
visit our Web site at www.books.elsevier.com

Printed in the United States of America
06 07 08 09 10 11 10 9 8 7 6 5 4 3 2 1

Table of Contents

Acknowledgments

There are many people I want to thank for the opportunity to write this book. They encouraged me and helped provide the opportunity and motivation to bring these thoughts to print. The list of supporters goes beyond the months of research, writing, and editing back over 25 years of customers, clients, and coworkers throughout the security industry. In their own way, each of them contributed to my education, and I will always be grateful for their praise, their criticism, and their suggestions.

But no one deserves my appreciation more than my wife Gail. Her constant unwavering support allowed me to do much of the hard work needed to understand how to do business in this industry. Regardless of the outcome of a bid or project, she was there to encourage me, celebrate the good times with me, and when times were not so good, remind me that there is always tomorrow. Gail deserves credit for any success this work may enjoy.

I am especially grateful to the members of ASIS International, Chapter 29, in New Orleans. I have been a member of the chapter my entire security career. To every member who ever said to me, "You should write a book about that...," I say, here it is. To all my fellow ASIS members, thank you for your support.

High praise is also due the membership of IAPSC (The International Association of Professional Security Consultants). After finishing the first draft, I asked the association members for their help and guidance in doing a peer review of the book. Their response was overwhelming. Their comments and critiques helped focus and fine-tune the work in a way that could never be done from a single perspective. These men and women helped me see what I took for granted, and they offered many useful new ways of communicating the right path to successful installations.

Special credit goes to these security professionals for their support and guidance during the peer review:

- Michael Brady, CPP, ABCP
- Ken Braunstein, MA
- Jim Broader, CPP, CFE, FACFE
- William Crews, CPP
- Mary Lynn Garcia
- Robert A. Gardner, CPP
- Harold C. Gillens, PSP, CHS-III
- Brian Gurin, PSP
- Freddie Lee, CFE, MA, PhD
- Ronald S. Libengood, CPP
- Steve Meyer
- John Sullivant, CPP, CHS-III [CMSGT, USAF RET]

This list would not be complete without thanking the editors at Butterworth-Heinemann for the faith in me and the potential of this work. This was my first book and they were taking a chance on its success. They deserve credit for having the vision to see the benefits of this work to the industry.

It is my fondest wish that security professionals everywhere embrace these techniques and that this book helps to bring much needed consistency to our industry.

Michael Khairallah, PSP

1 Introduction

WHAT IS THIS BOOK ABOUT?

This book is a comprehensive guide to identifying the man-made threats to an organization, determining the vulnerabilities of the organization to those threats, specifying security products to mitigate the threats and acquiring and implementing the recommended solutions. It represents the culmination of 25 years of experience in the design, installation, and project management of security system solutions.

The techniques in this book will help the security professional conduct a physical security audit to identify ways to mitigate identified threats and then specify a new security system or system addition to improve security conditions. The book also describes methods used in evaluating the survey data, proposing the recommended systems to company management, preparing a system bid, and managing the bid process. The book concludes with a description of project implementation and how to follow up the implementation to verify proper use.

The depth of detail in the book assumes the reader is a security professional and has some experience and the technical skill necessary to create a basic security system design. The book organizes the process and provides an overall structure for best practices in specifying system components and managing the acquisition and implementation process.

The main emphasis of this book is to provide the security professional with a guide for doing the right things at the right time throughout all phases of a physical security audit. It is an aid to planning and documenting the studies necessary to establish needs, and it outlines the tasks for acquisitions and implementation of systems to deal with threats. Even the experienced professional will find this book helpful in organizing the approach to security audit projects.

WHEN IS THIS BOOK MOST USEFUL?

This book is most useful when company management has recognized the need for improved security and requires a physical security audit to identify and mitigate threats. A physical security audit is just one component of a complete Risk Assessment. A Risk Assessment includes several disciplines and examines all elements of risk to the company's operation. Some additional areas of concern that are not covered in this book are:

- Data security
- Industrial espionage
- Relationships with local law enforcement
- Security protocol evaluations
- Disaster protocol evaluations
- Personnel assessments
- Building design and reinforcement measures
- Threats from internal sources, employees and service crews
- Terrorist threats

The most important milestone in beginning the physical security audit process is company management's recognition that the company needs security improvements. The security professional must help build "institutional will" to proceed with system design and evaluation. Throughout the process, management agreement must

be part of implementing the new security system to provide funding and foster acceptance of procedural changes.

This book will provide clear and meaningful guidelines for determining threats, assessing vulnerabilities, selecting system components to accomplish security goals, choosing the appropriate vendor to supply components, and implementing those components into a cohesive effective security system.

WHY IS THIS BOOK IMPORTANT TO YOU?

This is a guide to planning a security system audit to help avoid making expensive mistakes. Security system acquisition requires considerable planning of system details, coordinating vendor activity and comprehensive and adequate documentation. The security professional must clearly communicate system objectives for the implementation to be a success. In most security systems, but especially in access controls systems, an incorrect diagnosis of a problem or the failure to document those findings properly can result in costly errors. By using the techniques in this book, the security professional will avoid many of the common mistakes experienced in security system implementations.

This book will also help establish acceptance standards for getting the job done. These standards will be useful for the company and for the vendors hired to perform the work. By providing standards in all security system projects, the company will save money and the project team will save time. Standards are essential for measuring vendor performance. Without appropriate standards, performance quality is just guesswork.

WHO SHOULD USE THIS BOOK?

Security system project managers will find this book most useful when confronted by a major project for the first time. This book will be an excellent guide to developing the security audit plan and strategy, performing the audit and conducting all the steps necessary to implement the recommendations of the audit. Even if the security system project manager has years of experience, this book will be useful in organizing the necessary steps—from identification to implementation.

Security directors who are not project managers will find this book especially useful. It will provide a step-by-step process for identifying threats and vulnerabilities, designing the right system to mitigate threats and implementing the solutions.

Using this book is not a substitute for the skills of a qualified security systems' consultant. The reader may find that the level of expertise needed to conduct the required surveys may not be within their experience. In these cases, this book will serve as a guide to working with a professional security systems' expert.

A good indication that a consultant is a qualified expert is the certification of "PSP" following their name. The ASIS International Review Board grants the PSP or Physical Security Professional designation and defines a PSP as:

> The Physical Security Professional (PSP) designation is evidence that an individual is "Board Certified in Physical Security." It is awarded based upon experience and passage of an examination that provides objective measure of an individual's broad-based knowledge and competency in physical security. Ongoing professional development is required in order to maintain the credential. The PSP is administered by ASIS International, the preeminent international organization for security professionals, with more than 33,000 members worldwide.

Additional information on the PSP designation can be found on the ASIS International website at *www.asisonline.org*. To find a qualified consultant, the reader is encouraged to contact the International Association of Professional Security Consultants (IAPSC). Their website can be found at *www.iapsc.org*.

Further, membership in IAPSC provides assurance of high ethical standards. The IAPSC requires a code of conduct for its members and states:

> This Code of Conduct and Ethics signifies a voluntary assumption by members of the obligation of self-discipline above and beyond the requirements of the law. Thus, it notifies the public that members intend to maintain a high level of ethics and professional service, and proclaims that, in return for the faith that the public places in them, the members accept the obligation to conduct their practices in a way that will be beneficial to society.

This code of conduct is supported by these guidelines:

A. General
   1. Members will view and handle as confidential all information concerning the affairs of the client.
   2. Members will not take personal, financial, or any other advantage of inside information gained by virtue of the consulting relationship.
   3. Members will inform clients and prospective clients of any special relationship or circumstances that could be considered a conflict of interest.
   4. Members will never charge more than a reasonable fee; and, whenever possible, the consultant will agree with the client in advance on the fee or basis for the fee.
   5. Members will neither accept nor pay fees or commissions for client referrals.
   6. Members will not accept fees, commissions or other valuable considerations from any individual or organization whose equipment, supplies or services they might or do recommend in the course of providing professional consulting services.
   7. Members will only accept assignments for and render expert opinions on matters they are eminently qualified in and for.

B. Professional
   1. Members will strive to advance and protect the standards of the security consulting profession as represented in this code of ethics.
   2. Members recognize their responsibility to our profession to share with their colleagues the knowledge, methods and strategies they find effective in serving their clients.
   3. Members will not use or reveal other consultant's proprietary data, procedures or strategies without permission unless same has been released, as such, for public (or all consultants) use.
   4. Members will not accept an assignment for a client while another consultant is serving that client unless assured that any conflict is recognized by and has the consent of the client.

5. Members will not review the work of another consultant who is still engaged with the client, without such consultant's knowledge.
6. Members will strive to avoid any improprieties or the appearance of improprieties.
7. Membership in the IAPSC is forfeited upon conviction of any felony or misdemeanor involving moral turpitude.
8. Members will never misrepresent their qualifications, experience or professional standing to clients or prospective clients.

C. Forensic
1. Members' fees will never be contingent upon the outcome of a case.
2. Members, when testifying, will carefully avoid taking the position of an advocate or appearing to take such a position; for justice requires the professional expert witness to be neutral with no personal interest in the outcome of the case.
3. If, after reviewing a case, it is apparent that the expert witness cannot provide testimony or assistance helpful to the case, the consultant will make this known to the client. If he withdraws from or his services are discontinued by the case, he will not testify for the opposing side unless compelled to by subpoena.
4. The consultant will not sign written opinions or affidavits prepared by clients. Testimony or report preparation, including the preparation of oral reports, will not occur until the consultant has performed a thorough evaluation of the circumstances, evidence, scene or other pertinent materials or places as he deems necessary to render a learned opinion.

D. Enforcement
1. Upon a formal complaint issued against any member of this Association or other person indicating a violation of any section of this Code of Conduct and Ethics, the Ethics Committee will investigate the allegations and make a recommendation to the Board of Directors regarding any disciplinary action to be taken against the accused member. Discipline may range from a formal reprimand and warning to a temporary or permanent suspension from the Association upon the discretion of the Board of Directors.

By knowing the steps involved in a professional security assessment and properly managed project, the company manager can work more closely with the professional to achieve superior results.

BEING A CONSULTANT

The security professional may be an employee of the company in need of a new physical security system or professional consultant. The security professional may also be an experienced security manager performing work for the first time as a consultant.

Regardless of the role the security professional, a fiduciary responsibility exists between the security professional and the company. That relationship requires that the security professional act in the best interest of the company and tempers those actions with consideration for all concerned. A good business deal is one where all parties feel that they have benefited from the transaction.

A security consultant's obligation is to help the company do business with the security marketplace. The primary mission is to identify needs, then provide physical security systems and procedures to the company that mitigate risks. Fairness and a sense of cooperation must prevail in all aspects of the project.

Remember that a security professional is a "business consultant" first and a specialist in the security industry second.

OVERVIEW OF THE SECURITY AUDIT PROCESS

It is important for all businesses to understand the risks that may affect current operations. Businesses need to understand what can threaten ongoing operations and how to mitigate those threats through protection of assets and insurance against loss. The goal is to minimize exposure to those situations that expose the business to loss.

A comprehensive Risk Analysis provides a way to better understand these risks and the steps taken to reduce and manage the risks more effectively. This approach employs a two step process; the probability of an event occurring and the likely loss should it occur.