# Strategic Security Management
# A Risk Assessment Guide for Decision Makers

by
Karim H. Vellani

ISBN 0123708974
Publication Pending by Elsevier: December 2006



© 2006 by Karim H. Vellani, CPP, CSC

# TABLE OF CONTENTS

# INTRODUCTION

If you picked this book up, you're probably looking for more than the beginner's guide to security. Strategic Security Management is unique in that it fills the need for a definitive text on security best practices, introduces the concept of analysis for security decision making, and discusses advanced threat, vulnerability, and risk assessment techniques that you can apply to your organization's security program. You'll learn how to enhance a security program using security metrics to gain a true understanding of the problem instead of relying upon gut instinct or anecdotal evidence. This book will also teach you how to use security metrics to select and implement countermeasures and fine tune the program to ensure constant improvement and continual effectiveness.

The primary reason I wrote this book is simple: After searching many online and offline bookstores, I couldn't find a book that went beyond the security basics in a practical manner. No doubt, you've read plenty of great books written by security practitioners and others written by visionaries and theorists, but there wasn't that one book which brought it all together. Thus, the goal of Strategic Security Management is to bridge the gap between theory and reality, so to speak, on data driven security and metric based security decision making. Security metrics are woefully lacking in our industry today, but are commonly used tools in other industries, including our cousins in the information technology security industry. With the goal of bridging that gap, Strategic Security Management is written for three groups of people: Security professionals; other professionals who are responsible for making security decisions; and security management and criminal justice students.

For security professionals, those that carry the titles of Vice President of Security, Security Manager or Security Consultant, Strategic Security Management expands upon the collective body of knowledge in our industry and provides you with a fresh perspective on the risk assessment process. It will also give you some food for thought on the more controversial and complex issues of our business.

Other readers who will benefit from this book are those professionals that do not hold a traditional security title, such as security director or loss prevention manager, but are nonetheless charged with protecting their organization's assets. Your title may be facility director or property manager. As long as you make the security decisions for your company, Strategic Security Management makes the decision making process easier.

Security management and criminal justice students will find that Strategic Security Management gives you some insight into the diverse business that is security. You'll read (or should I say skim?) many security books that will teach you the basics needed to perform entry level responsibilities in this industry. Conversely, this book provides you with the foundation needed to climb the next step up the corporate ladder.

For the most part, this book uses the term *security decision maker* to refer to anyone responsible for making decisions relating to security. The term, security professional, is also used when the issue under discussion is complex or a newer security concept. The structure of Strategic Security Management follows the standard risk assessment methodology, diagramed in Figure I-1, and adds some unique chapters that will help you constantly improve your security program.

Chapter 1, Data Driven Security, sets the tone for the rest of the book with its discussion of a relatively new security concept, using data to drive the security program. Security professionals, only recently, have started using quantitative data to determine appropriate security levels. This chapter provides some of that food for thought mentioned above as well as a "how-to" for developing security metrics.

Chapter 2, Asset Identification and Security Inventory, discusses the first two steps of the risk assessment process, the identification and categorization of organizational assets and the itemization of existing security measures. Critical assets, those that are integral to the organization's mission, are the focal point of the first half of this chapter, while three types of security measures are discussed in the latter half. Also included in this chapter is a list of definitions so we're all speaking the same language as we progress through the book.

Chapter 3, Threat Assessments, should be an exciting section for most readers…..well, as exciting as it gets for professional books. The goal of this chapter is to illustrate the dynamic nature of threats that organizations deal with on a daily basis as well as the high impact threats which we face less frequently, but can have a detrimental impact on the assets and organizations we protect.

Chapter 4, Crime Analysis, is a component of a comprehensive threat assessment and the first major expansion on the crime analysis methodology published in Applied Crime Analysis. I've learned a lot since I originally outlined that book in 1999 and the security industry has advanced further toward the data driven security concepts developed during the intervening years. If you read Applied Crime Analysis, you'll add to that

knowledge by reading this chapter. If you didn't read it, well, that's a dollar in royalties I didn't earn. Fear not, I included an overview of the original material for you before getting into the new stuff.

Chapter 5, Vulnerability Assessments, is the fourth step in the risk assessment process. Much like the rest of this book, this chapter presents material not found in any other security text. Basically, a "how-to" for conducting security surveys, this chapter also helps you put together a vulnerability assessment team and write effective vulnerability assessment reports.

Chapter 6, Risk Assessment, wraps up the process of assessing your organization's risk once you have identified the existing and emerging threats and the vulnerabilities at your facilities. Both quantitative and qualitative risk models are considered.

Chapter 7, Information Technology Risk Management, is a primer for physical security professionals and others who have never delved into the world of information technology. Contributing author, Nick Vellani, is a Certified Information Systems Security Professional (CISSP), a Certified Information Systems Auditor (CISA), and a Certified Security Consultant (CSC). Nick wrote this chapter specifically for us, physical security professionals, with limited experience with information technology and information systems security. It's an important chapter now that the information technology security and physical security industries are coming together through the process of convergence.

Chapter 8, Prevention, provides some insight into *why we do the things we do* in the business of security. Don't worry, while it does cover the theoretical foundation of security concepts, 9 out of 10 readers agree its not boring. Ever hear the term Criminal Mastermind? This chapter discusses the ideas cultivated by the Prevention Masterminds.

Chapters 9 through 12 discuss the three types of security measures used in the protection of assets. Chapter 9, Policies and Procedures, covers the different types of written documents used to support a security program and the importance of documentation.

Chapter 10, Physical Security, is written by Brian Gouin, a Physical Security Professional (PSP) and a Certified Security Consultant (CSC). Brian utilizes his vast technological experience to identify the function and application of physical security measures utilized in the security industry today. This chapter will help you select the effective measures for your security program.

Chapter 11, Deploying Physical Security Measures, covers (you guessed it) the deployment of physical countermeasures. Written by Karl Langhorst, a Certified Protection Professional (CPP), this chapter goes in depth into the implementation phase of a security program from an end user's perspective. Karl is a true professional and you'll get a lot out of his chapter.

Chapter 12, Personnel, discusses the most expensive component of any security program, the security force. This just might be the most debated chapter in Strategic Security Management in that I present some ideas that are contrary to what has been done for years in our business. You'll learn about metric based deployment of security officers, the pros and cons of using police officers for security purposes, and why we need to increase the level of professionalism among our line personnel.

Chapter 13, Project Management, was added to the book's topic list after working with other independent security consultants on some rather large projects. One of the toughest things to do for most independent consultants is to get out of the way of the guy designated as project manager. However, consultants are not the only audience for this chapter. It is written for any security decision maker charged with implementing a new security project or upgrading an existing one.

Chapter 14, Premises Security Liability, is written by Norman Bates, a well respected security professional and attorney. Norm is not like other lawyers, he's actually a pretty good guy. Some of you might be familiar with his company's on-going study, *Major Developments in Premises Security Liability*. If you are, then the concepts in this chapter may be familiar to you as he draws upon that work and others to help us understand the liability risks we face every day.

Chapter 15, Forensic Security, is written by my good friend Charles A. Sennewald. Chuck's name should be familiar to most security readers as he has written a lot of security books including two that are on the CPP reference list. He is also a Certified Protection Professional (CPP), a Certified Security Consultant (CSC), and founded the International Association of Professional Security Consultants (IAPSC). Needless to say, this chapter is worthwhile reading for security professionals, especially those who testify as expert witnesses or on behalf of their employers in premises security litigation.

Chapter 16, Ethics in Security, is written by James Clark. Jim is also a Certified Protection Professional (CPP) and has served on the IAPSC's Ethics Committee. Always up for a good ethical debate, Jim has strong feelings on

the subject and has shed some light on the practical side of business ethics, especially as it pertains to the security industry. This chapter will benefit not only the independent security consultant, but also those security decision makers that hire them.

So that's the overview, sixteen chapters of new concepts, food for thought on older security principles, and advanced techniques that I am confident will assist you in your job as a protector. Soon after Applied Crime Analysis was published in early 2001, I remember wishing that I had the ability to add material to that book in a timely fashion. Of course, it's hard to do that with a printed book. So for this book I decided to add a companion website, www.ssminfo.com, where I'll add links to other helpful resources and update the information as the industry marches forward toward data driven security. I may even add a message board so we can talk in real-time and let others join in on the fun. In the meantime, I set up a special email account for you to contact me. Feel free to reach me in cyberspace to discuss (or argue) a point in the book or if you think I should add something to the website. The email address is info@ssminfo.com.

One last thought before we dive into the first chapter….while researching this book, I sought out the wisdom of others and came across a quote by William O. Douglas which I think captures the essence of Strategic Security Management: "Security can only be achieved through constant change, through discarding old ideas that have outlived their usefulness and adapting others to current facts." I think that pretty well sums up the intent of this book. Grab a cup of java and read on….