Chapter 1

INTRODUCTION

WHAT THIS BOOK IS ABOUT

Before making assumptions about security assessments based on past experience, consider first that you are about to be introduced to an entirely different perspective on the subject in this book. To begin, it is helpful to understand the environment that shapes not only our daily routine but our strategic thinking as well. And in doing so we will embrace the ability to "think outside the box."

Assessing vulnerability and risk has certainly been part of our experience since the beginning of humankind. It was evident when the leader of the pack told his most trusted kin to "go live among them and report back all you see and hear" what the task was, what was its importance to the survival of the tribe, and what was the standard of performance expected. As tribal cultures developed into more sophisticated civilizations, pharaohs, kings, emperors, prime ministers, and presidents of nations built and maintained their dynasties and countries by exploiting the strengths and weak-

nesses of both friend and foe and in particular members of their immediate and extended family. Agents dispatched throughout the region and foreign lands became "trusted envoys." They swore to observe the societal lifestyle and economy of the targeted population; determine attitude, morale, and loyalty; assess the will of the people and the strength of the military; discover the makeup of the government and its short- and long-term intentions; and secretly report their observations, conclusions, and recommendations to no one but the leader who sent them.

Due to the well-executed strategies and intelligence gathered in these types of missions, wars have been won or lost, territories and countries defeated or conquered, people enslaved or freed, political aims achieved or failed, and elections or appointments gained or lost. History offers us an opportunity to learn about the nature of these past assessments—why they succeeded, why they failed—and hopefully make us wiser in the process. This includes adapting our own methodologies to meet the needs of modern times and modern threats.

WHY THIS BOOK IS IMPORTANT

This book helps with these objectives by presenting a comprehensive methodology for conducting security assessments of the nation's critical infrastructures. **The S^3E Security Assessment Methodology focuses on clearly identifying, measuring, and prioritizing security risk for high-threat environments.** For too long many executive managers and security directors have been intimidated by this task and either taken investigative shortcuts or postponed the security assessment for another day. Conversely, many managers and organizations complete their assessments but still do nothing by way of strategic security planning. They report that embracing a comprehensive security strategy is not feasible due to impending obstacles, or they refute the security issues identified, believing they are not at risk. Others are very much aware of their facility's shortcomings but lack either the knowledge of how to proceed or the security budget to move forward. **The security-assessment methodology presented here provides a detailed roadmap that can help enterprises that are in denial of risk or lack an influential security director who can raise security standards and adopt protection planning.** Otherwise, in today's world of increasing vulnerability, such organizations are liable to become bad risk investments. Their business ratings and insurance premiums no doubt reflect this corporate culture or soon will.

The U.S. government does not perform comprehensive security assessments of all the national critical infrastructure sectors and key assets. Typically the owners or operators of infrastructure enterprises perform these assessments and mostly look to professional security consultants to carry out the task. Such assessments are important from both a local and a national planning perspective in that they enable authorities to evaluate the potential effects of a terrorist attack or other emergency on a given facility or sector and then invest accordingly in protection measures. Security assessments also serve as the building blocks for threat-vulnerability integration, allowing authorities to determine which facilities and sectors are at most risk. This aids local and national planners in developing thresholds for future standards for preemptive or protective action and setting priorities for changes to facility designs.

Enterprises [corporations, business organizations, government agencies, etc.] need to undergo systematic changes in their security posture as modern threats diversify and intensify and as the technical sophistication of terrorism increases with the availability of knowledge and materials to carry out acts of violence. World events have put terrorism at the forefront of the American psyche. These events and others have shown that terrorism in the U.S. is not about to end. In fact, it is only just beginning.

Various security-assessment models are currently in use, but many simply do not address the demands placed on business management. Some go partway but tend to introduce their own drawbacks and difficulties. They can be generic in nature or limited in scope and may only offer elementary guidance to a general audience. Others are neither consistent nor comparable in their methodology, thereby complicating protection planning and resource allocation.

Those sources that do offer a degree of useful detail are either government documents or private industry works with controlled distribution. For consultants who provide confidential security services to an array of clients, they can only access and use these sensitive materials under strict supervision and control and only when under contract for a specific project. In other instances, engineering firms, system integrators, and consultants have found it necessary to expand on works created by various professional associations and develop their own approaches. At best the data is scattered throughout the industry, forcing many security practitioners to research extensively to collect and assemble vital information. The most successful models are those that are performance-based, but many lack agreement on a best formula and outcome. **This book is an attempt to establish a much needed industry standard for generating solid and thorough security assessments for a varied clientele.**

Also of importance is the environment in which security assessments are conducted. If not performed by qualified individuals with a full understanding of analytical and security principles, they can do more harm than good. Poorly conducted assessments are a waste of time and resources and can lead enterprises to take action that is ineffective and may give them a false sense of security.

This book proposes to ease the research burden, develop investigative protocols for infrastructure assets, and pull together baseline data into a comprehensive and practical guide to help the serious reader understand advanced concepts and techniques of security assessment, with an emphasis on meeting the security needs of the National Critical Infrastructure. At a time when the U.S. government and corporate America are spending billions of dollars on performing risk assessments, establishing an innovative, acceptable, and proven methodology is vital for the national-critical-infrastructure environment. This methodology expands on the work of others, bringing together the best methods, techniques, measurements, and collective expertise of many colleagues and other professionals in an effort to raise the performance bar for conducting security assessments.

In summary, this book is a critical contribution to the field of security analysis in several ways. It offers a series of integrated strategies to evaluate the effectiveness and efficiency of an entity's security program. It pulls together user-friendly data into a comprehensive and practical guide to help the reader understand and apply advanced analytical techniques. And it provides a proven methodology applicable not only to infrastructure assets but to other organizations as well.

WHO CAN BENEFIT FROM THIS BOOK

This book will be an excellent guide for serious security practitioners, specifically:

- CEOs, presidents, and VPs of critical infrastructure businesses
- Homeland Security officials
- Directors of security and security managers
- Business-continuity managers and Risk-management managers

- Facility, traffic-management, and warehouse managers
- Human-resources managers
- Safety managers and quality-assurance managers
- Architects and engineers
- Judicial and correctional professionals in responsible leadership positions
- IT professionals responsible for computer security
- Security-system integrators
- Security consultants
- Managers and supervisors with operational responsibility for critical infrastructure businesses
- Government and military personnel with security and intelligence responsibilities
- Professionals responsible for security operations, emergency services, and public relations
- Law-enforcement professionals
- Researchers and investigators in the behavioral sciences
- Forensic examiners in the fields of medicine, psychology, criminology, accident reconstruction, crime-scene reconstruction, criminal investigation, engineering, and risk analysis

The book will also serve as a valuable reference in the academic world for:

- Educators, professors, and instructors in relevant fields
- Curriculum-development professionals
- Upper-division undergraduate and graduate students pursuing security-analysis expertise
- Security-training academies

HOW TO USE THIS BOOK

The text is divided into five major sections presented in a logical learning sequence. It is best to approach the book in the order established, as each chapter presents essential principles necessary to understanding subsequent material.

Part 1. Understanding the Environment

Part I guides the reader through the purpose and use of this book and the specific elements of western cultures that attract terrorism.

Chapter 1, Introduction, sets the stage by discussing:

- What this book is about
- Why this book is important
- Who can benefit from this book
- How to use this book

In **Chapter 2, Environments that Influence the Security Assessment: Threats, Western Values, and the National Critical Infrastructure Sectors,** American values are contrasted with the terrorists' ideology. This chapter discusses:

- Western social values: strengths, weaknesses, fears, and aspirations
- Safeguarding western values, safeguarding American values, the American population
- America's Inherent Vulnerabilities: American Values in Contrast with Tyranny's Oppression
- The Importance of the National Critical Infrastructure Sectors
- The protection challenge
- The nation's most direct threats and consequences

Chapter 2 offers an understanding of the greatest current threats to America's economy and security. It presents the clear and distinct need for security assessments as the vital first link of effective protection and the management actions that must follow to enhance enterprise security. Without a strong understanding of environments that influence the security assessment, it is a useless tool in guarding against terrorist attacks, major disasters, and other emergencies.

Part II. Understanding Security Assessment

Part II guides the reader through a comprehensive description of the S^3E **Security Assessment Methodology**. This model was developed and improved over many years of research and experience. It has been successfully used in industry and government domestically and internationally across the entire spectrum of the infrastructure sectors, including

some of the nation's most highly classified one-of-a-kind national experimental resources; military air, land, and sea assets; and national intelligence facilities. Over 3,000 security assessments have been completed in 30 countries and 5 continents using this approach.

Chapter 3,The Security Assessment: What, Why, and When, introduces and discusses:

- Why perform a security assessment?
- What is the scope of a security assessment?
- When should a security assessment be performed?
- Which security-assessment model is best?

Chapter 4, Proven Security Assessment Methodology, introduces the ***S*^{3}*E* Security Assessment Methodology**'s architecture and elements, defines its purposes and objectives, describes the behavioral and physical sciences at play and the techniques employed in the process, and addresses the standards adopted to evaluate and measure success. This chapter discusses:

- The security-assessment challenge
- A proven security-assessment model and methodology
- The security-assessment methodology as a system-level performance-based approach to problem solving
- Distinct benefits of the *S*^{3}*E* Security Assessment Methodology
- Enterprise key security strategies
- Enterprise security performance strategies
- Enterprise key security operational capabilities
- Security-assessment measurement criteria

Chapters 5 through 10 identify how the security-assessment methodology is performed. The process consists of six independent and separate tasks that are bound together by significant interrelationships and dependencies.

Chapter 5, Task 1, Project Strategic Planning: Understanding Service Requirements, discusses:

- Project mobilization and start-up activity
- Site-investigation preplanning
- Planning, organizing, coordinating, project-kickoff meeting

- Attending and co-chairing project-kickoff meeting
- Reviewing available project information and conducting workshops
- Conducting interviews
- Documenting the entire security-assessment process

Chapter 6, Task 2, Critical Assessment: Understanding the Service Environment, discusses:

- Site and facility mission and services
- Facility configuration and layout
- Asset and resource identification and criticality
- Documenting the characterization process

Chapter 7, Task 3, Identify and Characterize Threats to the Service Environment, discusses:

- Developing a design-basis threat statement
- Identifying adversarial groups and their capabilities
- Identifying the range and levels of threats
- Assigning likelihood ratings to ranges and levels of threats to assets
- Assigning ranges of malevolent acts to adversary attractiveness
- Determining loss consequences and probability of occurrence

Chapter 8, Task 4, Evaluate Program Effectiveness, discusses:

- Evaluating the status of operational systems, functions, processes, and protocols
- Evaluating the status of the overall security program including physical, operations, information, personnel security, and training
- Measuring program effectiveness

Chapter 9, Task 5, Program Analyses, discusses:

- Finalizing and refining the design-basis-threat profile
- Assessing vulnerability
- Determining and finalizing rank order for protection
- Developing workable solutions

Chapter 10, Task 6, Reporting Security Assessment Results, discusses:

- Developing enterprise-security strategies
- Developing mitigation solutions and cost estimates to implement program enhancements
- Presenting the report to executive management
- Presenting findings and recommendations to governing authorities

Part III. Tailoring the S^3E Security Assessment Methodology to Specific Critical Infrastructures

Part III provides the critical link for applying the methodology in diverse environments. The security-assessment methodology introduced in Part II is presented with many faces and an equal amount of applications tailored to specific infrastructure sectors. It therefore relies heavily on the reader's comprehensive understanding and ability to successfully employ the basic security-assessment principles presented in Part II in an effective and efficient manner.

Chapters 11 through 21 focus on particular infrastructure sectors. The template initially introduced in Part I is reintroduced but tailored to address these infrastructures:

- **Chapter 11. The Water Sector**
- **Chapter 12. The Energy Sector**
- **Chapter 13. The Transportation Sector**
- **Chapter 14. The Chemical Industry and Hazardous Materials Sector**
- **Chapter 15. The Agriculture and Food Sector**
- **Chapter 16. The Banking and Finance Sector**
- **Chapter 17. The Telecommunications Sector**

Chapters 11 through 21 are designed to stand alone, permitting the security analyst to concentrate on a particular sector with minimal reference to any previous chapter in Part II. To my knowledge, introducing such an integrated approach under one cover sets a new standard. It offers the diversified consultant, the security practitioner with multidiscipline responsibilities, and the academic the availability of a quick, reliable, and practical "briefcase" reference to use in the office as well as on the road.