Risk Analysis and the Security Survey
Dedication

To the memory of Mr. Murphy, who, God willing, waits for me at the Rainbow Bridge.
“If you don’t know where you’re going, any road will get you there.”
—Lewis Carroll, *Alice’s Adventures in Wonderland*
Contents

About the Authors   xv
Acknowledgments   xvii
Introduction   xix

Part 1. The Treatment and Analysis of Risk   1
1. Risk   3
   What Is Risk?   3
   What Is Risk Analysis?   4
   Risk Assessment   4
   Risk Exposure Assessment   6

2. Vulnerability and Threat Identification   9
   Risk Identification   9
   Examples of the Problems of Identification   11
   Security Checklist   12

3. Risk Measurement   21
   Cost Valuation and Frequency of Occurrence   21
   Principles of Probability   23
   Probability, Risk, and Security   25
   Estimating Frequency of Occurrence   27

4. Quantifying and Prioritizing Loss Potential   29
   Assessing Criticality or Severity   30
   The Decision Matrix   31
5. **Cost/Benefit Analysis** 33
   - System Design Engineering 33
   - Building Redundancy into the System 36
   - A Security Countermeasure 37

6. **Other Risk Analysis Methodologies** 39
   - National Infrastructure Protection Plan 40
   - Review 44

7. **The Security Survey: An Overview** 45
   - Why Are Security Surveys Needed? 45
   - Who Needs Security Surveys? 46
   - Attitude of Business Toward Security 48
   - What Can a Security Survey Accomplish? 49
   - Why the Need for a Security Professional? 50
   - How Do You Sell Security? 50

8. **Management Audit Techniques and the Preliminary Survey** 53
   - Audit Guide and Procedures 53
   - The Preliminary Survey 58
   - Summary 63

9. **The Survey Report** 69
   - “I Must Write, Therefore I Shall” 69
   - Five Criteria of Good Reporting 72
   - Format 75
   - Summary 78

10. **Crime Prediction** 79
    - Analysis of Internal Crime 80
    - Analysis of External Crime 81
    - Inadequate Security 85
How to Establish Notice 87
Review 89

11. Determining Insurance Requirements 91
   Risk Management Defined 91
   Risk Control 92
   Crime Insurance 92
   K & R (Kidnap and Ransom) Coverage 94

12. Emergency Management – A Brief Introduction 101
   Comprehensive Emergency Management Standards 103
   Private Sector Preparedness Accreditation and Certification Program 104
   National Incident Management System (NIMS) 104
   The Incident Command System (ICS) 104
   Unified Command 109
   Emergency Operations Center 110
   Summary 112

13. Mitigation and Preparedness 113
   Mitigation 113
   Preparedness 130
   Summary 133

14. Response Planning 135
   Emergency Response Planning and Response Plans 136
   Emergency Response Team 139
15. Business Impact Analysis  
   Risk Analysis versus Business Impact Analysis  203  
   Business Impact Analysis Methodology  204  
   Other Questions for the Impact Analysis  214  
   Resource Questionnaires and Forms  215  
   Summary  221  

16. Business Continuity Planning  
   Why Plan?  224  
   The Planning Process  225  
   Project Management  226  
   Summary  245  

17. Plan Documentation  
   Required Elements of the Plan  247  
   Multihazard Functional Planning  248  
   Plan Organization and Structure  249  
   Summary  257  

18. Crisis Management Planning for Kidnap, Ransom, and Extortion  
   Threat Identification  261  
   Plan Documentation  262  
   Plan Activation  263  
   Crisis Management Team  264  
   Handling the Initial Contact  266  
   Ransom Considerations  267
Preventive Security
Suggestions for Kidnapped Individuals
Media Control
Summary
Bibliography

19. Monitoring Safeguards
   Monitoring or Testing the Existing System
   The Scientific Method
   Five Basic Types of Testing
   Avoid Predictable Failure
   Some Audit Guidelines
   Develop a Plan of Action

20. The Security Consultant
   In-House versus Outside Advice
   Why Use Outside Security Consultants?
   Security Proposals (Writing and Costing)
   Summary
   Evaluation of Proposals and Reports

Appendices
   Appendix A   Security Survey Work Sheets
     General Questions before Starting a Survey
     Number of Employees
     Cafeteria
     Credit Union
     Custodial Service
     Company Store
<table>
<thead>
<tr>
<th>CONTENTS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Petty Cash or Funds on Hand</td>
<td>293</td>
</tr>
<tr>
<td>Classified Operations</td>
<td>293</td>
</tr>
<tr>
<td>Theft Experience</td>
<td>293</td>
</tr>
<tr>
<td>Some Reference Materials</td>
<td>303</td>
</tr>
<tr>
<td>Annex A: Hospital Surveys</td>
<td>303</td>
</tr>
<tr>
<td>Annex B: University and College Surveys</td>
<td>306</td>
</tr>
<tr>
<td>Appendix B  Sample Kidnap and Ransom Contingency Plan</td>
<td>309</td>
</tr>
<tr>
<td>I.  Introduction</td>
<td>309</td>
</tr>
<tr>
<td>II. Basic Plan</td>
<td>309</td>
</tr>
<tr>
<td>Appendix C  Security Systems Specifications</td>
<td>323</td>
</tr>
<tr>
<td>Introduction</td>
<td>323</td>
</tr>
<tr>
<td>Example: Requirements Specification for an Integrated Electronic Security System</td>
<td>325</td>
</tr>
<tr>
<td>Conclusion</td>
<td>327</td>
</tr>
<tr>
<td>Index</td>
<td>329</td>
</tr>
</tbody>
</table>
About the Authors

James F. Broder, CFE, CPP, FACFE, has more than 40 years experience in security and law enforcement. He has worked as a security executive, instructor, and consultant as well as having served in Vietnam as a Police Advisor in the Counter Insurgency Directorate, Vietnamese National Police. A former FBI Special Agent and employee for the US State Department, U.S. House of Representatives, Washington D.C. Mr. Broder is considered to be one of the most highly respected security authorities in the United States.

Eugene Tucker, CPP, CFE, CBCP, CHST is the head of Praetorian Protective Service®, LLC, and a past member of the board of directors of the Business Recovery Managers Association. He has served as the coordinator of the Emergency Management Program at a major University, and his professional interests and experience range from Security and Safety Management to Business Continuity Planning.
Acknowledgments

The first edition of *Risk Analysis and the Security Survey* was published in 1984. The book continues to be widely accepted within both the security profession and the academic community worldwide. Originally written for security and risk management professionals, it has become widely accepted as a textbook in Security Management degree programs in universities throughout the English-speaking world. Accordingly, we have tried to continue to meet the needs of our principal reading audiences and at the same time expand the text to keep pace with current trends in the world as viewed by security and law enforcement professionals. In this regard, the second half of this text, written by coauthor Gene Tucker, addresses the subjects associated with recovery. It is important to point this out because when security fails, as it occasionally does, recovery becomes paramount and security professionals must understand the vital role they play if they are to fully meet their responsibilities.

Security, once regarded by many in management and government as a necessary evil, has become recognized as a means necessary to combat evil. The events since September 11, 2001, have changed our outlook regarding the vital role security plays in protecting our national interest. We are no longer complacent. We recognize that an attack upon our facilities and infrastructures can occur at any time, in any place. It will be a long time before we are ever again allowed the dubious luxury of resting on our laurels.

One of the little-known ironies of the attack on the World Trade Center (WTC) was the recognition by the New York Port Authority Management that the WTC was to remain a prime target for another terrorist attack. The first attack occurred in 1993, which put WTC management on notice that security had to become a prime concern. Among other things, the security department was given an almost unlimited budget to upgrade the existing security countermeasures and “harden the target” to avoid a repeat of the earlier attack. One month before the 9/11 attack, the former Assistant Director of the FBI for Counter Terrorism, John McGuire, retired from the FBI to head the security staff at the WTC. John McGuire had personally led the investigation into the terrorist bombings of the three U.S. embassies in Africa and the attack against the Navy destroyer U.S.S. *Cole* in the harbor at Yeman. John McGuire was the Bureau’s leading expert on international terrorism. John McGuire and his staff of security professionals were all on duty that fateful morning in September when two aircraft were flown into the twin towers of the WTC. He, as well as all the members of his security staff and thousands of others, died on that unforgettable day!

So we would like to take this opportunity to acknowledge the great sacrifice made by John McGuire and the countless other security and law enforcement professionals who
have dedicated their lives to the cause of freedom in an effort to provide us with a more secure future. For many years before 9/11, John McGuire and others tried to warn us about the threat posed by international terrorists. How sad that he and so many others had to die to really get our attention.

The events of September 11, 2001 have taught us some valuable lessons:

We in security are about probabilities and not guarantees.

The enhanced security countermeasures put in place at the World Trade Center as a result of the 1993 terrorist bombing were more than adequate! The failures that occurred that fateful morning in security were at locations hundreds of miles from the WTC.

John McGuire and the security professionals from the New York Port Authority should rest comfortably knowing that they more than met their responsibilities, because the failures in the system that occurred did not occur at their location on their watch.

James F. Broder
San Marino, CA
In the early 1980s, we wrote the first edition of this book for the combined audiences of risk managers and security professionals. At that time, this author was employed as a security consultant for one of the largest insurance brokerage firms in the world. One of my early challenges was to explain to insurance brokers and their clients, risk managers for Fortune 500 companies, exactly what security professionals could do to reduce their risk regarding criminal and security issues. Risk management professionals were long accustomed to working with fire protection (property) consultants and safety (casualty) consultants. Few risk managers, however, had ever employed the services of a security professional. What gave rise to the need for property and casualty consultants was the necessity for clients to meet strict code requirements in order to be eligible for insurance coverage. Those requirements then, and now, were set forth in the form of “standards.” The National Fire Protection Association (NFPA) and the Occupational Health & Safety Administration (OSHA), among others, have published standards that are accepted by the insurance industry as the minimum standards required by an insured in order to receive consideration to become insured against the risk inherent in fires and accidents.

In California, fire protection and safety consultants are required to be licensed as Professional Engineers (PEs). We are not aware that security consultants have to be licensed in any state.

The two obstacles that had to be overcome were (1) the absence of standards in the security profession and (2) the fact that anyone could be a security consultant without regard to licensing requirements. The lack of published standards in the security industry exists to this day. While no state requires a security consultant to be licensed as a professional engineer, the security industry does have the “Certification” by the American Society for Industrial Security (ASIS), which has educational and testing requirements, generally accepted by risk managers and other insurance professionals as proof of professional competence.

The issue of the absence of “standards” in the security profession is paramount! Standards are the hallmark of most professional associations and societies. Why is this important for security professionals? Because standards set forth minimum requirements (benchmarks), which can then be used in auditing one’s security organization and program. As an example, this author has been engaged as an “expert witness” in many litigation matters (lawsuits regarding third-party liability). Invariably, the question I am often asked is, “What are the standards involved?” My usual answer is that we don’t have many standards in the security profession; what we have, instead, are “acceptable practices.” Another answer is, “Standards are whatever the client says they are!” Lawsuits involving the actions of security guards are very common. California, among others, licenses security guards. Regulatory requirements for licensing are often mistaken for standards by otherwise educated and experienced attorneys and judges. And in many cases the client or end users of security manpower and hardware do not have a clue about what does or does not constitute standards.

In 1980 we wrote, “The Risk Management Journal reported that 85 percent of those polled (Risk Managers) indicated that risk identification and evaluation was their number one priority.” We suspect that this figure has not changed much over the past 30 years. Risk Analysis
in this time has evolved as a methodology commonly used in the security industry. While we have not conducted a poll, there have been many articles written in security journals over these past years suggesting that the first order of business for security professionals is to fully identify their problems.

Readers of the earlier editions of this text will recognize that the material in Chapters 1–6, while updated, has not been significantly changed. The methodology we suggested in these chapters 30 years ago has stood the test of time. And, while the principles we suggest be used to perform a risk analysis are not categorized as “standards,” they have nevertheless gained wide approval as “acceptable practices.”

Accordingly, coauthor Gene Tucker and I once again set out here in the fourth edition to make a small contribution to the field of security. Granted, much has changed over the past 30 years. For one thing, the security profession has finally gained its rightful place, along with fire and safety, in the field of protection. Nevertheless, there is still much to be learned, and there will be continuing challenges for us in this profession to face. In this regard we urge the readers of this text to remember the basics. Spending time and using precious resources on the more glamorous but least likely harmful events that may occur is not serving the needs of our clients. International terrorism is a serious issue. However, the fact of the matter is that most of our clients have a greater chance of being struck by lightning than being attacked by terrorists.

James F. Broder, CFE, CPP, FACFE.

Similar to the security profession, the management of emergency and disaster situations is often guided by beliefs that are rooted in misunderstanding, misdirection, and mythology. Too often we believe and accept the mistakes or misconceptions repeated over and over by colleagues or, worse, by the media. Instead, we should turn to the research of social scientists and skeptically examine what we have done in the past or are encouraged to do in the future.

Careful attention to our text should point the reader in a direction that allows an effective analysis of potential events to reveal their true risk, highlight interdependencies, and understand that a single event can cause a cascade of failures or disasters. Consider as illustration the recent earthquake in Japan that caused a tsunami that interrupted power to a major nuclear power station and consequently affected the supply chain for the remainder of the world, not to mention the well-being of the environment and the surrounding population.

We have encountered more than one senior manager of an organization who has said that risk and business impact analysis is a useless exercise because a true manager is already aware of the issues, and, if they know their business, they don’t need risk analysis or business continuity planning. Those who think a security program or a business continuity plan, once in place, is sufficient without keeping it alive should speak with the survivors of a coastal community in Japan that was completely swept away by the 2011 tsunami. The great majority of the population survived. Many believe this was because they identified the risk and analyzed it until they had a firm understanding of the problems they faced. They practiced tsunami evacuation on a regular basis. The managers mentioned above have looked at us with a “deer in the headlights” expression when the risk or business impact analysis revealed a serious exposure that they had not anticipated.

According to the British philosopher Herbert Spencer, “There is a principle which is a bar against all information, which is proof against all arguments and which cannot fail to keep a man in everlasting ignorance—that principle is contempt prior to investigation.”

Gene Tucker, CPP, CFE, CBCP, CHST