THE SCIENCE AND TECHNOLOGY OF COUNTERTERRORISM

Measuring Physical and Electronic Security Risk

Carl S. Young

B
H

The Science and Technology of Counterterrorism

Measuring Physical and Electronic Security Risk

Carl S. Young

ELSEVIER

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

Butterworth-Heinemann is an imprint of Elsevier

Acquiring Editor: Pamela Chester
Editorial Project Manager: Marisa LaFleur
Project Manager: Punithavathy Govindaradjane
Designer: Russell Purdy

Butterworth-Heinemann is an imprint of Elsevier
225 Wyman Street, Waltham, MA 02451, USA
The Boulevard, Langford Lane, Kidlington, Oxford, OX5 1 GB, UK

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

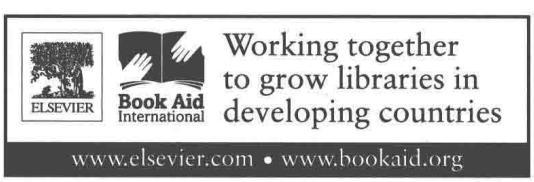
Library of Congress Cataloging-in-Publication Data
Application submitted

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

ISBN: 978-0-12-420056-2

Printed and bound in the United States of America
14 15 16 17 18 10 9 8 7 6 5 4 3 2 1

For information on all Butterworth–Heinemann publications
visit our website at *http://store.elsevier.com*



The Science and Technology of Counterterrorism

Dedication

To my nieces and nephews, Claire Melin, Julia Melin, Harry Uniman, and Max Uniman

Acknowledgments

With respect to acknowledgements, I am most indebted to my parents, Dr. Irving Young and Dr. Geraldine Young. In addition to their continued love and support, they encouraged me to take the "road not taken" in the words of Robert Frost. In that vein, I am thankful that I chose not to follow in their footsteps, and became a physicist rather than a physician.

Other individuals have played a disproportionate role in the creation of this book, and they are noted below.

The first such individual is Mr. Jean Gobin. He contributed significantly to the material on electronic security risk in Chapter 8 and the section on virtualization in Chapter 9. Jean is one of the most talented and knowledgable electronic security professionals in the business. I am indebted to him for his contributions to this book as well as for his efforts in support of the Security Science group at Stroz Friedberg.

My longtime colleague, friend, and mentor, Dr. David Chang, deserves mention. Dave performed the heavy lifting on the probability of protection method applied to explosive threats, the results on window protection from ballistic and explosive loading and the calculation of the passive RFID field magnitudes specified in Appendix G. I have had the privilege of learning from Dave for over 25 years as well as bearing witness to his humility that belies his exceptional scientific talent.

Jim King was a colleague when we both worked for our respective governments. Jim emerged from fighting the forces of evil for Her Majesty to face the more daunting task of being my boss at Goldman Sachs. In his capacity as Global Head of Physical Security, he encouraged me, and others, to think expansively about security. Many of the ideas explored in this book originated while working for Jim. I hope he finds this book "helpful."

Roger Pike, President of RPA Ltd. in the UK, is another key security figure that directly and indirectly contributed to this book. Roger has an encyclopedic knowledge of physical security technologies, and also possesses a remarkable problem-solving capability. In my view he has no equal as a physical security expert on either side of the Atlantic.

Chris Hogan and I met relatively late in the evolution of this book, but he nonetheless had a significant impact. He and I spent months together in Pittsburgh, Pennsylvania and Portage, Indiana (of all places). During this time I had the privilege

of learning from a truly iconic security practitioner. Moreover, he gave me encouragement and inspiration to complete this journey, and I am indebted to him for his knowledge, wisdom, and friendship.

I am most appreciative of the support provided by various individuals at Stroz Friedberg, LLC. Specifically, Ed Stroz, who befriended me when I arrived from Washington in 2000. We were both escapees from government service, and he made me feel at home in my newly adopted city. I recall our many dinners at Gus' Place (now extinct) in the West Village with fondness. In 2011 he gave me the opportunity to start a security consulting practice at his company, possibly because he became bored with hearing me complain about security consultants. I am grateful for that opportunity as well as his continued friendship and support in writing this book. I would also like to acknowledge Bob Lynch, Chief Financial Officer. Our brainstorming sessions over lunch at Walker's in TriBeCa have been an important source of nutrition, mentally and otherwise.

If this book is successful, it will largely be due to the efforts of the team at Elsevier. They toiled long and hard behind the scenes, and managed to overcome the many hurdles I consistently if unintentionally placed in their way. Specifically, I am most grateful to Pam Chester (acquiring editor), Marisa LaFleur (editorial project manager), Punithavathy Govindaradjane (project manager), and Russell Purdy (designer).

I happened to have the good fortune to have worked with the Cyber Security team at United States Steel while writing this book. This team of bona fide security-risk professionals includes Andrew Blasko, John Eshenbaugh, Tom Lentz, Caryn Mckenna, Stephanie Sjoberg, and Nicole Trimbey. I was inspired by their dedication and unwavering enthusiasm as exemplified by their signature greeting, "Carl! Good to see you!!"

The Security Science team at Stroz Friedberg is a remarkable collection of technical talent. I have never worked with a more knowledgeable group of security professionals and I am indebted to them for all they have taught me. Contributions from specific individuals are interspersed, and so acknowledged, throughout this book. Team members as of this writing include Chris Briscoe, Chantnu Chandel, Dave Dalva, Steve Doty, Kendra Garwin, Jean Gobin, Nitai Mandhyan, Steve Ruzila, and Dominic Spinosa.

Finally, readers of this book will definitely note my bias in applying statistics to all types of phenomena. But the laws of probability alone cannot fully explain how one family suddenly appeared and altered my perspective on risk and reward. So I must acknowledge their contribution to this book without adequate explanation, but with profound appreciation nonetheless. Family members in order of seniority include Josefina Quinn, Mariana Ramirez, Michael Kowalski, and Aidan Quinn.

There are many others I have not mentioned because of space limitations or I have acknowledged previously. I am fortunate to have many friends and acquaintances to whom I am personally and professionally indebted. I sincerely hope they are not offended by not being mentioned by name.

About the Author

Carl S. Young has specialized in applying science and quantitative methods to problems in security risk management. He was a Supervisory Special Agent and Senior Executive in the FBI as well as the Global Head of physical security technology at Goldman Sachs & Co. in New York, and Goldman Sachs International in London. He is currently the head of the Security Science consulting practice and Chief Security Officer at Stroz Friedberg, LLC in New York City. He is also an adjunct professor in the Protection Management Department of the John Jay College of Criminal Justice, City University of New York (CUNY).

Mr. Young was a consultant to the JASON Defense Advisory Group, and was selected by the Director of Central Intelligence to advise the intelligence community on technology as part of a blue ribbon panel. In 1997 he was awarded the James R. Killian Medal by the White House for individual contributions to national security. He is the author of *Metrics and Methods for Security Risk Management* (Syngress, 2010) as well as numerous technical papers related to security risk management. Mr. Young received undergraduate and graduate degrees in mathematics and physics respectively from the Massachusetts Institute of Technology (MIT), Cambridge, MA.

Preface

This is my second book on security risk management. In *Metrics and Methods for Security Risk Management*, I examined the individual components of risk for a variety of physical security threats. I also discussed the importance of identifying the risk factors that affect those components of risk. This book expands on those themes, and there is admittedly some duplication in specific areas.

However, I had different objectives in writing this book, and therefore this is a very different work. In both books I provide a framework for security risk assessments. This is fundamental to addressing counterterrorism issues from first principles and to developing truly strategic solutions.

But in this book I hope to create a comprehensive reference that is useful to practicing security professionals. To that end, I specify the theory that underpins fundamental security controls, and importantly, how theory affects implementation. The focus is clearly on technology controls related to counterterrorism, but I include other methods that apply to more general problems in security.

The main objective of this book is to teach the reader how to think *strategically* about security risk management by understanding fundamental security principles and methods. I also provide supporting technical details to enable the application of those principles to realistic terrorism scenarios. Anyone can memorize a list of widgets and technical specifications. When security technologies are viewed as controls that affect the overall security risk profile, the development of a risk-based strategy is possible.

To that end, the risk assessment framework specified in Chapter 1 is a recurring theme throughout this book. This is because it provides the rationale for every counterterrorism control discussed thereafter and is essential to developing a risk-based mitigation strategy. Although it is a relatively simple framework, examples are always helpful. I therefore provide numerous examples gleaned from actual security scenarios. Such examples also illustrate the practical limits on controls that are often imposed by Mother Nature.

In some cases these examples may seem a bit esoteric. I might indeed agree, but sometimes it is valuable to stretch the limits of the imagination in thinking about security. Our field can be constrained by templated thinking and the reflexive use of checklists. There is a benefit to thinking about security in nontraditional ways.

Chapters 2 and 3 discuss tools that could be used to "measure" security and counterterrorism risk. The word measure is in quotation marks because the results are typically estimates; exact measurements of security risk are frequently elusive. The importance of uncertainty in terrorism is also explained, and this includes a discussion on random variables. Ironically, the assumption that a risk factor is a normally distributed random variable introduces a degree of certainty to the inherently uncertain world of counterterrorism.

It is important to know how security technologies work mainly because it is relevant to evaluating their effectiveness in addressing risk. Understanding threats on a scientific level is also important, in part because it is the science that often dictates the magnitude of the vulnerability component of risk. Moreover, scientific and risk-based explanations of security threats and mitigation technologies are typically absent from traditional security references or are presented in nonsecurity-related contexts. When such concepts are not coupled to security issues they can seem too abstract to be useful.

In that vein, simple physical models are presented in Chapter 4 along with their application to broad classes of security problems. These models include point sources of radiation, exponentially increasing and decreasing processes, harmonic motion, and Gaussian plumes. In my experience these are most useful in performing "back of the envelope" calculations to yield order of magnitude estimates of security risk. Such estimates also provide a valuable reality check on intuition.

Chapter 5 provides a unique method of examining risk. Specifically, the risk factors of various threats are assumed to be normally distributed random variables. What evolves from this assumption is a means of determining the likelihood of the effectiveness of security controls. This is fundamentally different than calculating the likelihood of a future terrorist incident, a typically fruitless endeavor.

Chapter 6 is devoted exclusively to analyzing the risk associated with conventional explosive threats. Understanding how such threats scale, i.e., change, with distance and payload is central to estimating vulnerability. As always, specifying the risk factors for a given threat or attack vector is essential to developing an effective risk mitigation strategy.

Chapter 7 discusses "nontraditional" terrorism threats. These include radiological, chemical, biological, and electromagnetic pulse weapons. The models

discussed in Chapter 4 are used to develop a realistic if coarse estimate of the vulnerability to these threats and the effectiveness of controls.

Another key objective of this book is to provide a deeper understanding of electronic terrorism risk. The distinction between electronic terrorists and other "cyber" criminals may be mostly semantic. However, in Chapter 8 the focus is on electronic threats that might have particular appeal to a terrorist, based on the potential damage inflicted and/or headlines achieved through such an attack. Detailed analyses of relevant controls and how they address common modes of attack follow discussions of the threats themselves. With respect to controls, emphasis is placed on monitoring inter-zone network traffic in the spirit of "measuring" risk in this context.

Importantly, in Chapter 9 there is a detailed discussion on the increasing convergence of physical and electronic security risk. In that discussion, specific physical security system components with potential electronic vulnerabilities are identified in addition to showing how physical vulnerabilities facilitate electronic attacks. This convergence is often mentioned in security literature but the details are sometimes missing. Absent information showing where and how this convergence occurs, such treatments do not convey a full appreciation of the risks.

Providing the proper balance between theory and practice is important in a book that strives to be useful for both practitioners and academics. Chapters 10, 11, and 12 cover the fundamental controls of physical security. The treatment is risk-based with explanations grounded in science and augmented by quantitative analyses. Physical access control systems, sensors, and CCTV are discussed in detail as well as their application to various counterterrorism scenarios. A statistical treatment of security device/sensor performance is also presented, an analysis that is in keeping with a more quantitative treatment of risk.

The theoretical foundations of threats and technologies are central to understanding risk, but as noted above, a key objective is to provide a useful reference for security practitioners. Therefore, I attempt to identify "rules of thumb" and simple performance metrics associated with security technologies. These are approximations that are useful in quickly assessing risk and/or in performing back-of-the-envelope calculations of system performance. The pixel density for CCTV systems immediately comes to mind. Numerous tables with security technology specifications are included that are useful in examining risk, and which are particularly handy when compiled in a single reference.

Although some readers might be put off by the occasional mathematical excursions, I believe the game is worth the chase. These may also save the day the next time you are asked for a more rigorous justification of a security-related expenditure. Hopefully you will agree, and thereafter view security risk management in a more analytic light.

Problems are provided at the conclusion of each chapter. These are intended to test the student's grasp of the fundamental concepts. Many of these problems derive from real-life scenarios and I often attempt to put the reader in the shoes of security decision-makers. Despite my occasional attempt at humor, it is important to keep in mind that decisions made by security professionals can have significant consequences. All problems are tightly coupled to the concepts imparted in the text. In my view this is essential in order to satisfy the book's objectives.

Finally, I must comment on terrorism itself. Terrorism has become useful to politicians, and is sometimes invoked to further nonsecurity-related agendas. Those in power get to determine who is a terrorist and who is a legitimate defender of the realm. Dictators are fond of labeling opponents who favor democracy as terrorists.

Security professionals are obliged to demonstrate more integrity and intellectual rigor than politicians, which fortunately is not difficult. There is a science to measuring security risk, and that is what this book is all about.

"The most important questions of life are indeed, for the most part, really only problems of probability."

Pierre-Simon Laplace
(Théorie Analytique des Probabilités: 1812)

Contents