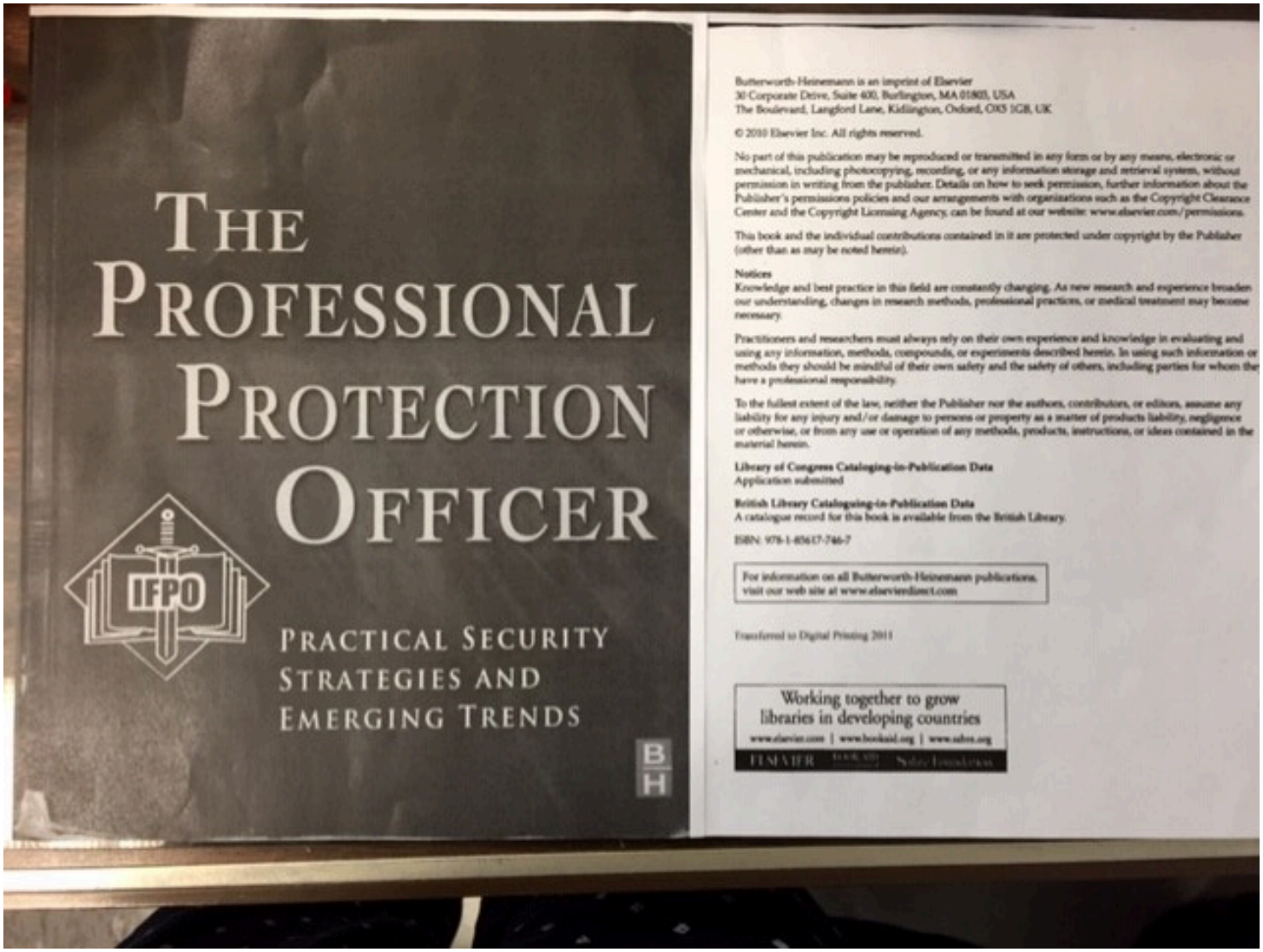


Butterworth-Heinemann is an imprint of Elsevier
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
The Boulevard, Langford Lane, Kidlington, Oxford, OX5 1GB, UK

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

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments 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: 978-1-85617-746-7

For information on all Butterworth-Heinemann publications, visit our web site at www.elsevierdirect.com

Transferred to Digital Printing 2011

Working together to grow libraries in developing countries
www.elsevier.com | www.bookaid.org | www.sabre.org
ELSEVIER BOOK AID Sabre Foundation

CHAPTER

27

Security Risk Management

Kevin E. Peterson

CHAPTER OBJECTIVES

- Explain the basis for all protection functions, regardless of environment in which they are practiced
- Identify and define two key elements of security risk management
- Explain the risk management cycle/process
- Reinforce the idea that the practice of risk management requires both a thorough risk assessment and an ongoing program of risk monitoring
- Provide the tools to apply security risk management strategies to assess a situation, develop a menu of feasible options, and recommend a realistic solution set to meet defined asset protection objectives

THE HISTORICAL BASIS FOR RISK MANAGEMENT

The idea of "risk" and "risk management" is not unique to the security field—in fact, it is relatively new to us. The idea probably originated in the financial industry, where risks can result in significant loss of money or missed opportunities to grow financial assets. In recent years, financial risk has been highlighted by major losses in worldwide financial markets and public scandals such as the Enron collapse (2001) and the Bernie Madoff fraud case (2008). In fact, Madoff's scheme has been described as "the biggest financial swindle in history" (Frank & Efrati, 2009).

Concern for managing risk is also critical in other fields such as business, science and technology, politics, and insurance. In reality, some degree of risk is inherent in almost any business decision. Should we develop a new product line? Establish a joint venture or partnership with a particular company? Manufacture or distribute our products in a different country or region of the world? Expand the business? Build a new facility? The answer to any one of these questions can result in tremendous growth for a company and its revenues—or it can mean disaster (in business terms).

If we think about these questions from our perspective, however, we can see that the answers usually have security risk implications as well. Because of this, it is extremely important that security professionals be included in discussions over important business or organizational decisions.

The same can be said of fields such as scientific research and development and the application of new technologies. Almost any program or project decision in these areas can have significant implications for the future—including security and asset protection issues. As an example, consider the selection among various ballistic missile defense technologies for the United States. This is clearly an issue of technology risk when comparing such diverse options as ground-based interceptors, space-based interceptors, the airborne laser and seaborne platforms. Besides the obvious factors of cost, schedule, and performance, each of these approaches also has security implications. Think of how to go about developing a security approach to protect the people, equipment, communications, and information associated with each of these options. This will probably show quite different security challenges and recommendations for each platform.

Finally, the insurance industry is almost entirely focused on the concept of "risk." In fact, one of the earliest uses of the term "risk manager" is attributed to companies that recognized the increasingly clear relationship between business practices and insurance costs in the 1950s (Thompson, 2003). The role of risk management in the insurance industry is further illustrated by the fact that in 1975, the American Society of Insurance Management changed its name to the Risk & Insurance Management Society (RIMS) (Hampton, 2007). Essentially, the insurance providers are taking on (or accepting) a portion of their policy holders' risk for a fee (their premiums). As we will discuss later, insurance is the most common example of "risk transfer," one of the five avenues of addressing security/asset protection risks.

WHAT IS SECURITY RISK MANAGEMENT?

So how do we (protection professionals) fit into the picture of risk management? As mentioned in an article by Diana Thompson, a well-respected consultant in organizational risk management based in Australia:

> To most businesses, the concept of risk management is confined to financial aspects ... but the risk game is fast changing ... [now] covering everything from a computer meltdown to a terrorist attack... (Thompson, 2003)

Today, risk management is a central concept in the fields of security, asset protection, and crime/loss prevention. Risk management principles are used to help us conserve our limited resources (in terms of time, effort, manpower, and money), apply the right solutions in the right places, and keep up with changes in our operational environment. Plus, as shown in the quote above, it keeps us attuned to the broad array of threats that we face in any type of organization.

TWO KEY ELEMENTS: ASSESSMENT AND MITIGATION

The practice of security risk management (SRM) begins with a thorough and well-thought-out risk assessment. Why? Because we cannot begin to answer questions until we know what the questions are—or solve problems until we know what the problems are. A good assessment process naturally leads directly into a risk mitigation strategy. These two key elements will be discussed further in this chapter and are mentioned at various points throughout this book with respect to specific protection applications.

Note: The following material is extracted from "Primer on Security Risk Management" and is used with permission.

Whether in the public or private sector and whether dealing with traditional or cyber security (or both), asset protection practice is increasingly based on the principle of *risk management*. The concept is a perfect fit for the field

of asset protection, since our primary objective is to *manage* risks by balancing the cost of protection measures with their benefit.

TAKING A STRATEGIC RISK MANAGEMENT APPROACH

Too often, organization leaders look for the "quick fix" to satisfy their security needs. They buy a popular security system or are convinced by a sales representative that a particular product or service is the all-encompassing answer to their protection needs. They are convinced that their critical assets are then completely safe without even asking what those assets are or what types of threats they face. This is a particular problem for small and medium-sized businesses, but it certainly could apply to any size enterprise.

Taking a "strategic approach" means basing the enterprise's asset protection practice on sound *planning, management, and evaluation*, and taking into consideration both the organization's mission and the environment in which it operates. A "strategy" should articulate—to the security professional and executive decision makers—*what* is being protected, *why* it's being protected and *how* it's being protected.

The National Infrastructure Protection Center (NIPC)[1] defines *risk management* as "a systematic and analytical process by which an organization identifies, reduces and controls its potential risks and losses." They further state that risk management:

- Identifies weaknesses in an organization or system.
- Offers a rational and defendable method for making decisions about the expenditure of scarce resources and the selection of cost-effective countermeasures to protect valuable assets.
- Improves the success rate of an organization's security efforts by emphasizing the communication of risks and recommendations to the final decision-making authority.
- Helps security professionals and key decision makers answer the question, "How much security is enough?"

(National Infrastructure Protection Center, 2002)

THE RISK MANAGEMENT PROCESS

The five components of the risk management process—which lead to a comprehensive asset protection strategy—are depicted in the accompanying diagram (Figure 27-1). The process begins by identifying realistic asset protection objectives and then conducting a comprehensive risk assessment (described below). This can be done at the enterprise-wide level and/or at the specific process or project level. Depending upon the nature of the business, it may be appropriate to do it at multiple levels.

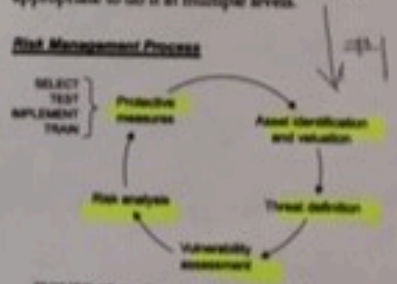
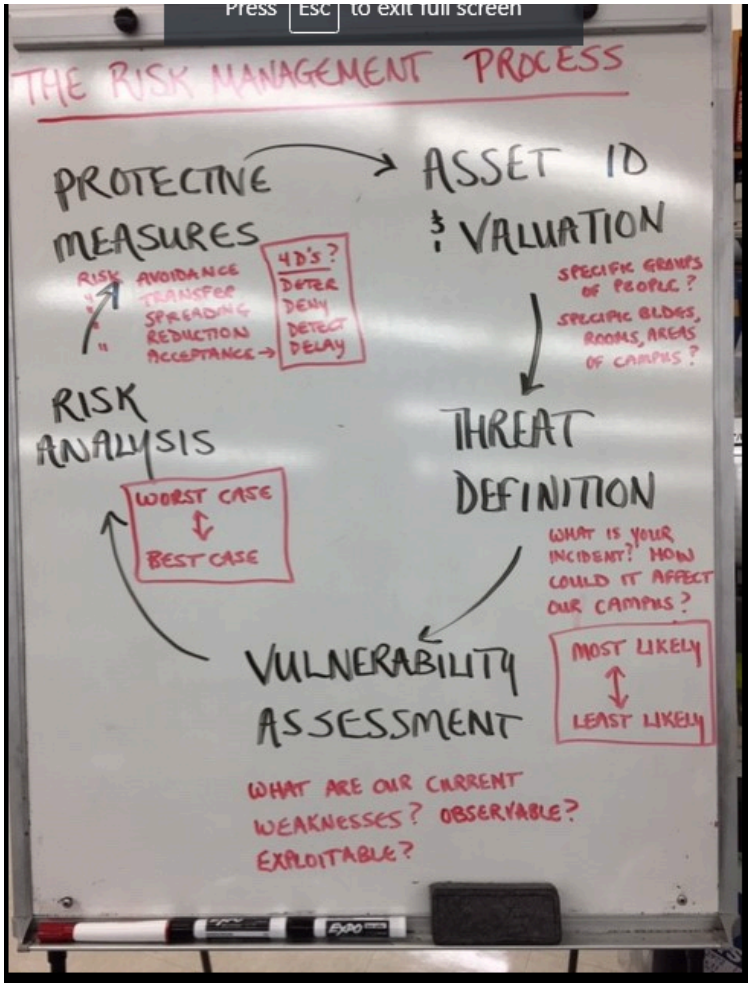


FIGURE 27-1 The risk management cycle

[1] With the establishment of the Department of Homeland Security (DHS) within the U.S. government, the responsibilities of the NIPC were redistributed between the DHS Information Analysis and Infrastructure Protection (IAIP) Directorate and the FBI's Cyber Division.


Press Esc to exit full screen
THE RISK MANAGEMENT PROCESS
PROTECTIVE MEASURES
RISK AVOIDANCE
TRANSFER
SPREADING
REDUCTION
ACCEPTANCE
4D's?
DETER
DENY
DETECT
DELAY
ASSET ID & VALUATION
SPECIFIC GROUPS OF PEOPLE?
SPECIFIC BLDGS, ROOMS, AREAS OF CAMPUS?
RISK ANALYSIS
WORST CASE
BEST CASE
THREAT DEFINITION
WHAT IS YOUR INCIDENT? HOW COULD IT AFFECT OUR CAMPUS?
VULNERABILITY ASSESSMENT
MOST LIKELY
LEAST LIKELY
WHAT ARE OUR CURRENT WEAKNESSES? OBSERVABLE? EXPLOITABLE?