CHAPTER

1

Introduction: Why Security and Risk Management Matters

What is this book about?

In this book, readers will learn how to understand, analyze, assess, control, and generally manage security and risks from the personal to the operational.

Security, as described in Chapter 2, is, essentially, freedom from negative risks. Risks, as described in Chapter 3, are the potential returns (consequences, effects, etc.) of an event. Risks are inherently uncertain, and many people are uncomfortable with uncertainty, but security and risk management is a practical skill set that anyone can access. Readers of this book do not need to learn theory or many facts but will be introduced to the processes by which security and risks can be managed and to the contexts of many real risks. Readers will be left informed enough to start managing security and risks for themselves or to further investigate the subject.

We all should care about better security and risk management because, if done well, we would live in a more secure and less risky world. Awareness of risk is entirely healthy, because everything we do is literally risky; by simply interacting socially or undertaking any enterprise, "everyone willingly takes risks" (Adams, 1995, p. 16).

Unfortunately, not all security and risk management is conscious or sensible. People tend to obsess about certain risks and ignore others or manage risks in distorted ways that discredit the whole practice of management. Unfortunately, in the past, security management and risk management were routinely separated, with all sorts of disciplinary and professional incompatibilities, but security and risk management are complementary and properly tackled together.

Public expectations for security continue to grow, but sensitivity to certain risks and dissatisfaction with their management also continue to grow. In the last two decades or so, official and private authorities—international institutions, governments, trade associations, general managers, employers, contractors, and employees—have formally required better management and specified how it should be delivered, stimulating more disputes about proper definitions and practices.

This book provides a new practical guide to the proper synthesis of security and risk management.

Private Requirements for Security and Risk Management

Outside of government, private citizens and managers of commercial activities want or are expected to take more responsibility for their own security. For instance, public authorities urge private citizens to prepare for emergencies at home, to consult official advisories before they travel, and to rely less on public protections. Commercial organizations reserve more internal resources or acquire their own protections after finding public protections or private insurers less reliable. Managers of projects, operations, information, acquisitions, and human resources now routinely include security or risk management within their responsibilities. According to Gary Heerkens, "Risk and uncertainty are unavoidable in project life and it's dangerous to ignore or deny their impact . . . Risk management is not just a process—it's a mindset" (2002, pp. 142, 151).

Public Attention to Risk

Security is a primary responsibility of government, which acquires militaries, police forces, coast guards, border protections, health authorities, and various regulators to ensure the security of their territory and citizens. By the 1970s, public authorities managed security and risks mostly in the sense that they managed public safety and controlled crime. For instance, in 1974 the British legislated in favor of a Health and Safety Executive, passed new legislation protecting employees, and increased public entitlements. However, these actions failed to control other risks, such as terrorism, and encouraged inflated views of some risks, such as workplace risks (which have declined), while neglecting other risks, such as sexual risks (which have increased). Even where risks have not increased in any real sense, societies have developed into *risk societies* that show increased sensitivity to risk in general, though they neglect or activate certain hazards, such as environmental hazards, due to misplaced attention to some risks over others (Beck, 1995; Beck, Ritter, & Lash, 1992; Wisner, Blaikie, Cannon, & Davis, 2004, pp. 16–18).

Requirements for Better Management

The increased salience of both security and risk is indicated by the shift in United Nations (UN) operational management from an official objective of *safety and security* to *security risk management* (since 2005), followed by the Humanitarian Practice Network's similar objective (2010). A publicly accessible online tool (http://books.google.com/ngrams) suggests that use in books of the terms *risk*, *security risk*, *international risk*, and *global risk* grew over the last three decades by several orders of magnitude each and peaked around 2006 (the data runs out in 2008).

Increased attention to security and risk does not always produce better management of security and risk. The requirement for wider security management is often met by narrower sets of skills. Requirers could outsource to specialist security or risk management contractors, but some of these providers have betrayed their clients with superficial skills and even ethical or legal violations. For instance, in February 2013, the U.S. Government unveiled a civil lawsuit, following similar suits by several states and the District of Columbia, alleging that a risk rating agency had defrauded investors by supplying ratings of the risks of financial products that were not as independent as the agency had claimed.

Organizations usually lack a manager trained to manage risks across all domains and levels, although general managers may have some training. Organizations often assign corporate responsibilities for risk

management to their finance, information, or project managers, who should offer some generalizable skills in security management or risk management, although each domain has peculiar risks and a particular approach. Financial risk management and project risk management are not perfectly transferable and have suffered crises of credibility since the latest global financial crash (2007–2008).

Project risk management is tainted by repeated official and corporate failures to manage the largest acquisition projects. Information managers also often lead corporate risk management, but national governments continue to complain about growing information insecurity. Meanwhile, many corporations are in the habit of hiring former law enforcement or intelligence officials as security or risk managers, but their particular skills usually do not extend to generalizable skills in security and risk management.

Criminologists generally "maintain that security is a subject that has yet to be adequately covered by any specific discipline or in a satisfactory interdisciplinary fashion" (Van Brunschott & Kennedy, 2008, p. 18). Even in practices and professions of relevance (such as policing), security and risk management is not necessarily a focus, as noted in the following:

> The wide array of risk-related concepts shows how deeply embedded these ideas are in our thinking about crime. Yet, relatively little effort has been made to sort out the different meanings of risk and their importance for analyzing criminal events . . . It is also the case, as we will demonstrate, that criminologists have spoken about and understand risk as an element of crime. Interestingly enough, in their discussions of risk, these analysts have tended to treat risk lightly, rarely incorporating it explicitly into their studies of motivation, opportunity, or prevention (although, of course, a large part of the field is attuned to the ideas of risky lifestyles and rational choices based on risk). (Kennedy & Van Brunschot, 2009, pp. 10, 12)

Official Standardization

Some of the dissatisfaction with security and risk management has prompted more standardization, in the hope that the many competing and loosely defined ways in which people manage security and risk can be replaced by the best ways. Standardization is the process of defining standards for behavior and understanding. Standards describe how concepts should be understood and how activities should be performed. Standardization certainly helps interoperability and accountability and may replace inferior practices with superior practices.

Over the last few decades, more international authorities, national authorities, trade associations, and private corporations have developed standard practices for managing risk and security and for describing their management of security and risk to each other. From the late 1980s, after comparisons with the apparently superior performance of the private sector in delivering services or acquiring items as planned, democratic governments started to escalate the importance of risk management and standardized how their agents should manage risks, initially mostly in the context of the acquisition of capabilities. For instance, in 1989 the U.S. Defense Systems Management College issued guidance on risk management. In 1992, the British Ministry of Defense (MOD) started to issue *risk guidelines*. In both cases, the emphasis was on defense acquisitions.

In 1995, the Australian and New Zealand Governments issued their first binational risk management standard, which was adopted by or influenced many other governments, including the British, Canadian, and U.S. Governments. However, the latter three governments continue to negotiate between

international standards and departmental standards, effectively negotiating between those who prescribe one standard and those who prefer decentralized choice. In a large government, specialized departments can justify different effective standards, but differences interfere with coordination, and some standards can be inferior, not just different. Some of the highest departments still contest basic concepts of security and risk, with consequences for assessments and treatments on the scale of billions of dollars. The United Kingdom, Canada, and the United States have dealt with enormous risks and intercepted some spectacular threats but continue to reveal inadequacies in their security and risk management, most observably during the management of defense, homeland security, information security, and diplomatic security.

All three governments are disproportionately involved in building the capacity of foreign governments, but most governments have effectively elevated the Australian/New Zealand standard for risk management to a common standard of which new versions were published in 1999, 2004, and November 2009, the last version endorsed by the International Organization for Standardization (ISO). In practice, subscribing departments often adapt the standard for their own purposes and have struggled with parts of the standard, but at least they have a common source.

In the United States, any of the Government Accountability Office (GAO), Department of Homeland Security (DHS), Department of Defense (DOD), or Department of Treasury could be the U.S. Government's center of excellence for security or risk management. Even the Congressional Research Service has taken a role in critiquing and thence developing how departments manage security and risk. The Federal Bureau of Investigations (FBI) and Central Intelligence Agency (CIA) and the rest of the *intelligence community* have plenty at stake in security, not to mention other authorities at state, city, and local levels. These departments and their agencies, bureaus, and offices tend to internal standardization but are often in dispute. Elected officials have led many investigations and reports on official security and risk management, often with very peculiar understandings of security and risk.

In the Canadian Government, the Department of National Defense and Public Safety Canada (since 2003) are the leading coordinators of military security and civilian risk management, respectively, although other departments lead the management of particular risks. Neither has a mandate to order other departments to manage security or risk in certain ways, although Public Safety Canada issues guidance and encouragement to other departments. Public Safety Canada tends to admit the ISO standard but has adapted parts and continues to adapt it, with primarily British and Dutch influence. The Canadian police forces have no national standard setting authority, although the national association—the Canadian Association of Police Boards—has developed risk policies, and the Canadian Police College teaches risk management to police executive and board members. The Royal Canadian Mounted Police (the federal police service) and the Ontario Provincial Police each has a risk management policy and a risk group. Municipal police forces are governed by provincial laws and overseen by police boards or commissions, none of which has standardized risk management, although some, such as those in Edmonton, Alberta, and Toronto, have formal risk management policies and practices.

In 1997, the British Treasury, under the direction of the Cabinet Office, published guidance that required the government to assess the risks of all project and program options and specifically warned against past overoptimism. Before the year was out, the Treasury required statements on Internal Financial Control (which official commissions had recommended to commercial companies in previous years) from all departments starting fiscal year 1998 to 1999 and issued guidance on controlling fraud. In February 2000, the Treasury first circulated guidance on the management of risk for use by all of government; in December, it required from all departments of government by the end of the

2002/2003 fiscal year "a fully embedded system of internal control" of risk (U.K. Treasury, 2004). In August 2000, the National Audit Office (NAO) issued best practices gathered from mostly the private sector; in November, the British Standards Institution (BSI) published its guidance on *corporate governance* and *internal control*. Also in 2000, the MOD mandated both a risk management plan and a risk management strategy to its own standards for all acquisitions projects. By the 2000s, official efforts refocused on increased hazards like weather storms, diseases, and terrorists. In July 2001, the British government established the Civil Contingencies Secretariat, responsible for business continuity across government and for policy for planning the response to national emergencies. The Prime Minister's Office (2002) published as policy a declaration that risk management is "central to the business of government." In 2004, the Treasury (p. 9) reminded government that "[r]isk is unavoidable, and every organization needs to take action to manage risk in a way which it can justify to a level which is tolerable." The Treasury reported that "government organizations now have basic risk management processes in place" (2004, p. 11) but stopped short of standardization across government. Even though the British executive formally advocated more international cooperation in the assessment and management of international risks (Strategy Unit, 2005, p. 15), it has not formally adopted international standardization. The British Standards Institution and private British organizations have published standards for simultaneous private and public use but generally conform with the ISO (see: Association of Insurance and Risk Managers, ALARM The National Forum for Risk Management in the Public Sector, & the Institute of Risk Management [AIRMIC, ALARM, and IRM], 2002, and BSI, 2000 and 2009), while the government has endorsed none for use government wide.

Benefits of Good Management

Security and risk management (at least when performed well) offers benefits: it improves security, strategy, resource allocation, planning, communications and transparency, and thereby confidence. The NAO sought to transfer commercial practices to government with the following promise:

> Risk management can help departments improve their performance in a number of ways. It can lead to better service delivery, more efficient use of resources, better project management, help minimize waste, fraud and poor value for money, and promote innovation. (2000, p. 4)

The Australian/New Zealand standard promised the following example benefits:

1. Increased likelihood of achieving objectives;
2. Proactive management;
3. Awareness of the need to identify and treat risk throughout the organization;
4. Improved identification of opportunities and threats;
5. Compatibility of practices;
6. Compliance with relevant legal and regulatory requirements and norms;
7. Improved financial reporting;
8. Improved governance;

9. Improved stakeholder confidence and trust;
10. Reliable base for decision making and planning;
11. Improved controls;
12. More effective allocation and use of resources for controlling risks;
13. Improved operational effectiveness and efficiency;
14. Enhanced health, safety, and environmental protection;
15. Improved management of incidents;
16. Reduced losses;
17. Improved organizational learning;
18. Improved organizational resilience. (2009, pp. iv–v)

One private study found that Fortune 1,000 companies with more advanced management of their property risks produced earnings that were 40% less volatile, while the other companies were 29 times more likely to lose property and suffered 7 times costlier losses due to natural causes (F.M. Global, 2010, p. 3).

This Book

The aim of this book is to give practical knowledge of and practical skills in the management of security and risk. The managerial skill set is practical, with analytical skills in understanding the sources of risk, some basic mathematical methods for calculating risk in different ways, and more artistic skills in making judgments and decisions about which risks to control and how to control them.

This book introduces the skills and gives the reader different tools and methods to choose from. These skills are multilevel and interdisciplinary. Readers are shown not only, for instance, how to defend themselves against terrorists but also how to identify strategies for terminating the causes of terrorism or to co-opt political spoilers as allies.

In this book, readers will learn how to

- understand, analyze, and assess security and risk;
- understand and analyze the sources of risk, including hazards, threats, and contributors;
- understand and analyze the potential targets by their exposure and vulnerability;
- understand and assess uncertainty and probability;
- understand and assess the potential returns of an event;
- develop an organization's culture, structure, and processes congruent with better security and risk management;
- establish risk sensitivity and tolerability and understand the difference between real risk and perceived risk;
- control risks and select different strategies for managing risks;

- record, communicate, review, and audit risk management; and
- improve security in primary domains, including
  - operations and logistics,
  - physical sites,
  - information, communications, and cyber space,
  - ground, air, and maritime transportation, and
  - personal security.

Part 1 describes how to analyze security and assess security and risks back to the causes and sources through the relevant concepts: security and incapacity (Chapter 2), risk (Chapter 3), hazards, threats, and contributors (Chapter 4), target exposure and vulnerability (Chapter 5), uncertainty and probability (Chapter 6), and returns (Chapter 7).

Part 2 describes how to manage security and risk, including the development of or choice between different cultures, structures, and processes (Chapter 8), establishing tolerability and sensitivity levels (Chapter 9), controlling and strategically responding to risks (Chapter 10), and recording, communicating, reviewing, assuring, and auditing risk and security (Chapter 11).

The third and final part introduces ways to improve security in the main domains: operational and logistical security (Chapter 12); physical (site) security (Chapter 13); information, communications, and cyber security (Chapter 14); transport security (Chapter 15); and personal security (Chapter 16).