ELSEVIER

ELSEVIER'S SECURITY EXECUTIVE COUNCIL
RISK MANAGEMENT PORTFOLIO

THE MANAGER'S HANDBOOK FOR BUSINESS SECURITY

SECOND EDITION

GEORGE K. CAMPBELL, Contributing Editor

Security
Executive Council

THE SEC PROCESS

We walk clients through eight critical steps to reach their goals

The first step is an assessment of your current environment. What needs improving? What are Security's fixed conditions? What recent changes have impacted Security, such as new business directions, new stakeholders, or a merger or acquisition?

An SEC team made up of former CSOs will engage with you to identify the key risks and determine the continuum of desired outcomes depending on your conditions. We map the solution to your C4R – current circumstances, conditions, culture and resources.

Once we understand the issues and potential barriers, we search our extensive security knowledge base for resources or research data that can be used as a base or to kickstart direction ideas.

Next, our subject matter experts bring their varied experiences and knowledge together to create a plan to help you reach your desired outcome. We call this Collective Knowledge™.

We help determine which other functions the plan should touch and align with. We use the SEC's Unified Risk Oversight™ model to help plan and communicate the value of cross-functional collaboration.

We assist in communicating the value of the project to the business leader accountable for Security's new vision. This in turn assists in communicating the strategy to senior executives from other functions.

Business value metrics are developed for the client team to measure and determine project success for the organization, including key stakeholders.

Last, clients can either take the SEC deliverables and run with them, or we can guide you through the implementation of your plan. At the end of the day, **the SEC is here to help you succeed.**

The SEC Process Outcome: Security Leader and Program Success

Elsevier
225 Wyman Street, Waltham, MA, 02451, USA
The Boulevard, Langford Lane, Kidlington, Oxford, OX5 1GB, UK

Originally published by the Security Executive Council, 2009

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
Campbell, George, 1942-
The manager's handbook for business security / George K. Campbell. – Second edition.
pages cm
ISBN 978-0-12-800062-5
1. Business enterprises–Security measures. 2. Risk management. I. Title.
HD61.5.C36 2014
658.4′7–dc23
2013045269

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

ISBN: 978-0-12-800062-5

This book has been manufactured using Print On Demand technology. Each copy is produced to order and is limited to black ink. The online version of this book will show color figures where appropriate.

CONTENTS

3

RISK ASSESSMENT AND MITIGATION

Introduction

If management, your directors, and insurers did not see the need to manage the types of risk they see—under your watch—you would not be here.

Business Value

Business unit management likely does not fully appreciate the depth and breadth of risk that you will understand. Your department's programs will enable the business to do what would otherwise be too risky. Measure and communicate that value.

The Essentials

Depending on the scope of your security responsibilities, there are several relatively common business-based vulnerabilities and risk exposures that you should consider in your risk assessment strategy:

1. Absence or weakness of effective business controls—combined impact of employee empowerment, business velocity, and growth on reliability of controls and effective care
2. Ethical lapses by employees in key positions—maintenance of reputation and avoidance of corporate liability
3. The corporation as a property owner—crime, workplace violence, and premises liability
4. Business interruption—failure to plan and be effectively prepared
5. Adequacy of logical and physical access controls—unauthorized access to our facilities and proprietary information
6. Connectivity and reliability of safeguards—the company's reliance on technology and critical pathways
7. Lack of business—process-based ownership of security

8. Globalization of the business—internationalization of risk
9. Corporate visibility—the company and key executives as high-profile targets
10. Inadequate focus on security-related risk—maintenance of awareness on risk dynamics

Assessing Viable Threats

You can find any number of well-done articles on threat assessment. The challenge is defining which threats are real for your organization now and based on where they are going in their evolving business plan. Threat assessment is a critically important product of the security organization, because nobody else has a clue, and no one is doing it in your space. On-line threat-reporting security resources are numerous, but they can only generalize and do little that is specific to your company, unless you have a tailored and contracted service at your disposal.

Threat is the source of the risk. The diverse threats confronting our businesses are dynamic, not static. They may be natural events beyond our control, man-made errors, accidents, or criminal acts, and there are deficiencies in your system of internal controls or other risky business practices. When we talk about threats, we often hear, *But it hasn't happened here*. This may be true, but as you see in Figure 3.1, there are incremental steps in threat likelihood, and the more exposed you are to *exploitable vulnerabilities*, the greater the likelihood of a threat

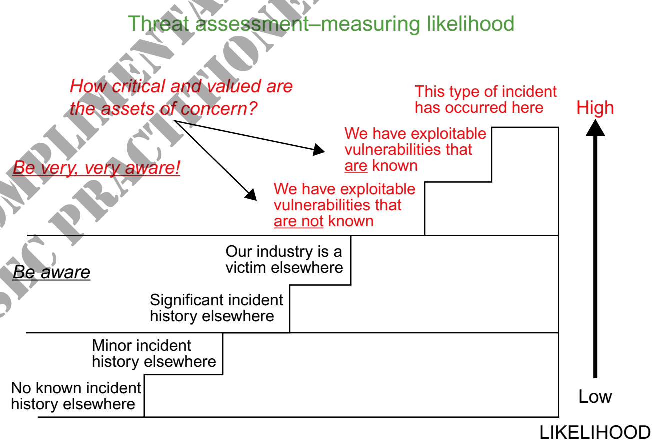

Figure 3.1 A representation of the incremental steps in measuring threat likelihood.

becoming a reality. That situation underscores the critical need for on-going risk and vulnerability assessments, with particular attention to the threat from the knowledgeable insider.

Vulnerability Assessment

Drilling down within risk assessment finds the real focus of a follow-up strategy: nailing down how exposed or vulnerable a critical process or asset is to compromise or loss. Vulnerabilities are flaws in protection that may be exploited by an adversary, or a set of conditions that contribute to protection system failure. If there is a single compulsory exercise for the asset custodian and the security team, it is to have an on-going program of identifying vulnerability to critical assets and business processes from specified threats. It's an interesting exercise to sit with a business process owner and ask, "If you wanted to [name the attack] this asset, how would you do it and avoid detection?" The incident post-mortem is an ideal opportunity to identify vulnerability with one very notable exception: *it's too late*.

Vulnerability is broad in scope and may be measured outright or with opportunities for compromise estimated. Building weaknesses are exploitable and measurable. Access to the asset (s) is measurable. Probability of detection is measurable. Protection systems can be disarmed, bypassed, or simply overlooked. People in key positions make mistakes, may be compromised, or have dishonest objectives of their own. If redundancies are not in place, you can measure the ability of employee response to pre-planned events. You can apply covert and overt tests to measure effectiveness of safeguards. In some cases, you may want to employ trusted outside experts to test your security measures under carefully controlled conditions.

Risk within business activities comes in many flavors. The keys to controlling these varied risks are to understand the source of the threat to specific assets, where the gaps in protection may be found, and what kinds of controls need to be in place to address these vulnerabilities and mitigate these risks.

> The probability of experiencing a major incident is primarily determined by the strength of the controls applied to an environment. —Information Security Forum

Board-Level Risk and Security Program Response Research

Enterprise risk assessments (ERA) are becoming more common. Soon, every major corporation will have conducted an internal review or will have engaged outside contractors to conduct an assessment. Inevitably, this assessment will be presented to the board of directors or the executive management team. Internal executives will be assigned to each risk and will be required to report periodically to the board on progress to mitigate the risk. This pattern is being repeated across the United States and across the globe, and both members and non-members of the Security Executive Council have observed it. The Council wanted to address this trend by creating a tool that members could use in presentations to the board of directors or senior management.

This project has resulted in a successful graphic representation of the board-level risks an organization may face, and the security processes and programs designed to mitigate them. The Board-Level Risk Diagram sample that follows (see Figure 3.2) facilitates executive management's understanding of board risk and the role security plays in reducing it.

The methodology employed involved numerous completed ERAs provided by both member and non-member companies, and several other ERA examples were found through research. All ERAs were analyzed for commonality, and their content was categorized into eight Council-identified board-level risk topic areas. Faculty and staff were asked to review the risk areas and report on any security programs or services provided to their companies, which would remove or reduce the board-level risk.

The Board-Level Risk Diagram can be modified to present the overall ERA security response to the board in a succinct and quickly understandable manner. The concept chart can also be used to quickly position the value of security on par with any other staff group addressing major risks to the corporation. It may also be used for staff and departmental training and awareness of the board-level risks, as well as the role the department plays removing or reducing them. For companies in which an ERA has not been completed, security directors have reported this chart has been effective in establishing security as a leader in identifying and communicating how departmental services add to board-level value.

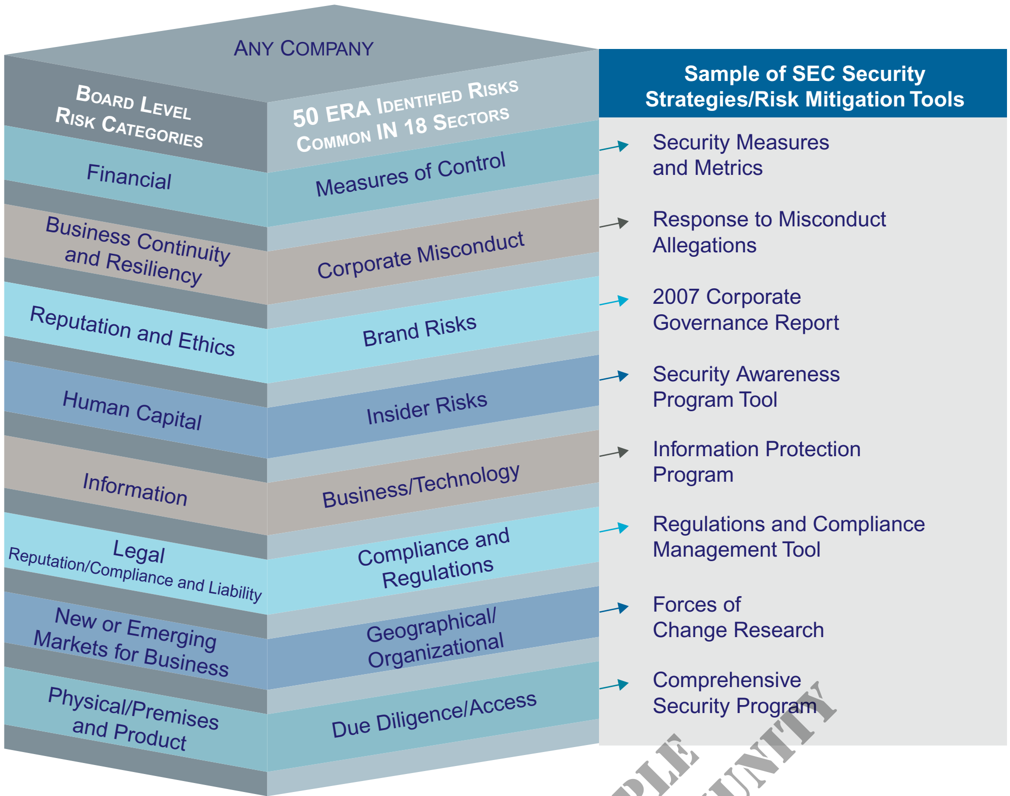

Figure 3.2 Solutions to Reduce Board-Level Risk. A graphical representation of the eight board-level risk categories.

A Risk Quantification Process

Having a list of security-related business risks and their associated countermeasures is an essential part of the risk management process. However, understanding how to quantify those risks to set priorities is equally important. The flow chart in Figure 3.3 lays out one approach to the analytical process associated with risk exposure quantification.

In Step 1 of the diagram in Figure 3.3, the process commences with an inventory of business risk information available from internal risk management (values and volume impacts, and insurance data), industry risk data, security's risk and hazard data, known incident data from all governance functions, and incident post-mortem outputs. These profiles enable selection of a more likely set of single-incident risk scenarios. Based on their unique consequences, you now have one or several types of incidents you can value.

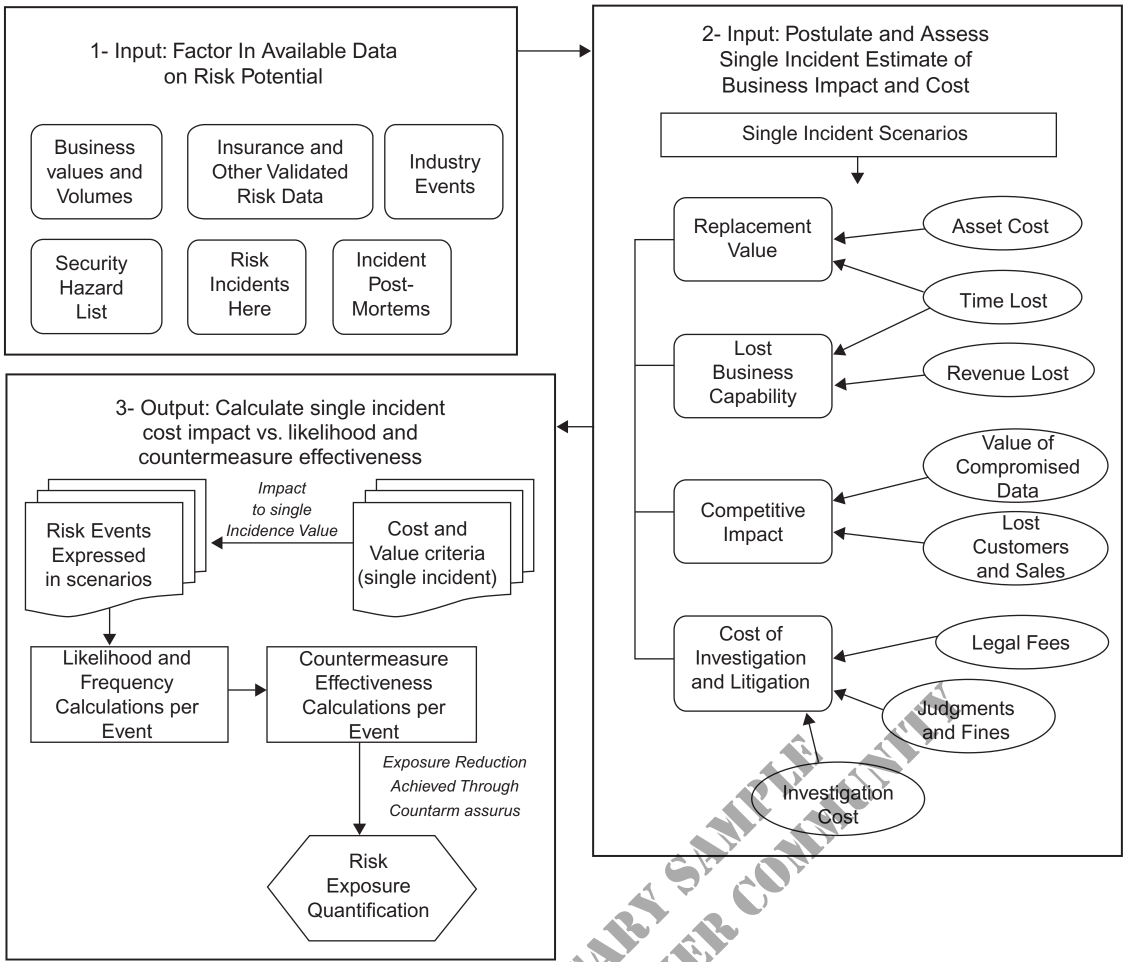

Figure 3.3 Risk Exposure Quantification Strategy—Process Flow. One approach to the analytical process associated with risk exposure quantification.

These scenarios are forwarded to the second step to postulate multiple factors related to the potential consequences and impact of a single incident of the specified type. Estimates of cost may be made for each scenario using a worst-case baseline, such as total loss of a known valued asset, or a less-consequential result, such as an outage for a specified time. Impact costs may be estimated by engaging the business unit, which typically has loss-impact data calculations as part of the contingency planning baseline. Other estimates may be merely logical plug-ins supported by prior-event data.

The single-incident cost estimates are then processed through the filter of the effectiveness of the countermeasures that are in place for each risk event. For example, backup resources are in place to respond to a natural disaster outage, and the time to recover may be reliably estimated through prior tests. That recovery time and other impacts may also be reliably cost estimated. You will find your CFO and risk management or insurance offices most helpful in identifying insurance industry data associated with various security incidents, scoping single incident costs to risk impacts, as well as approaches to potential cost to various security scenarios.

Likelihood of an incident is a measure of knowledge of your vulnerability to specific breaches based on test data, known downtimes, audit data on unresolved business process deficiencies, and increased frequency of similar events within your industry or nearby. Effectiveness of countermeasures is also based on test data. The known resilience or identified weaknesses of the countermeasures available in your scenario will drive your likelihood estimates. For example, what if this process were to postulate a much wider impact of the disaster that limited or eliminated the backup capability in our outage scenario above?

You will find that your best likelihood measure used for influential impact will be your periodic testing of the effectiveness of various safeguards applied by your resources and those employed within business units, particularly where they are required by standard or policy. Several key areas of measurement include:

- the perceived value or attractiveness of the object of protection;
- the degree of probable success in penetrating a specific countermeasure; and
- the greater the knowledge of that vulnerability within the population, the greater the likelihood of successful attack.

Each of these concepts may be verified by testing.

There are a variety of risk-quantification tools available through risk-management organizations and vendors. This is but one exercise that may be engaged in by a governance team approach or in cooperation with the potentially affected business units.

The bottom line is the need to understand the potential impact of the higher-likelihood risk events in financial and other relevant terms.

More in-depth discussions may be found in the ASIS International *General Security Risk Assessment Guideline*[1] and in the Institute of Internal Auditors booklet *Business Risk Assessment*.[2]

[1]ASIS International, Alexandria, VA, 2003.
[2]David McNamee, Institute of Internal Auditors, Altamonte Springs, FL, October, 1998.

The chart in Table 3.1, developed by Sandy Sandquist, director of global security at General Mills, provides an excellent way to spell out sets of risk scenarios and estimate impact in financial and operational terms. Use it to specify your estimate of risks appropriate to your assessment of likely exposure to the business. In this example, "High" is equal to or greater than $100 million; "Medium" is between $10 and $100 million; and "Low" is equal to or less than $10 million. Use different impact values to suit your own risk concerns.

A Risk Management-Based Concept of Operations

A simple and straightforward way to approach security risk mitigation is to think of it in three progressive levels: anticipation, preparation, and execution.

1. *Anticipation*—Risk is dynamic. Perhaps more than another business executive, the CSO is paid to anticipate risk, to think and understand "what if," and to have in place a credible program to qualify viable threats. This program involves the following elements:
   - the ability to maintain an actionable threat profile utilizing credible local and international resources and assets;
   - the ability to install and maintain an integrated set of security controls that provide real-time indications of risk—key risk indicators (KRIs);
   - the ability to *reliably* document and analyze security/risk events to identify and mitigate vulnerabilities and develop improved response capabilities that are tracked and monitored—key performance indicators (KPIs);
   - the ability to be thoroughly knowledgeable in the capabilities and competencies of security assets; and
   - the ability to attract and retain a customer-responsive cadre of protection assets.
2. *Preparation*—There are three ways we learn the presence of risk: (1) an unanticipated event; (2) we probed and discovered conditions that could result in an event, and we did not follow-up; and (3) we probed, discovered, and closed the gap. Credible anticipation imposes an obligation to be prepared for the "what ifs." Preparation involves, but is not limited to, the following:
   - the ability to influence the organization and its leadership so that response capabilities are in place and tested;

Table 3.1 Corporate Security Potential Impact/Cost

Corporate Security
Issues/Risks with Potential Impact Greater Than $X Million Prior to Any Mitigation Efforts

Major Issue/Risk	*Select Impact**	*Possible Outcome*
Catastrophic loss of key staff in single event	☐ High ☐ Medium ☐ Low	☐ Loss of key personnel ☐ Delay or loss of new product launch ☐ Lawsuits ☐ Loss of investor confidence
Terrorism—regional event	☐ High ☐ Medium ☐ Low	☐ Loss of use of business-critical facility and employee logistics ☐ Possible loss of employee lives ☐ Loss of regional workforce ☐ Evacuation of all nearby businesses/residences ☐ Long recovery time with major business interruption
Workplace violence	☐ High ☐ Medium ☐ Low	☐ Possible loss of employee lives ☐ Temporary interruption with certain products if facility is sole supplier ☐ Negative publicity ☐ Adverse litigation
Nationalization of operation (international)	☐ High ☐ Medium ☐ Low	☐ Loss of use of production facility ☐ If plant is sole supplier, out of market with certain products ☐ Loss of business with minimum compensation ☐ Loss of proprietary business process to competition
Product tampering resulting in death or serious injury	☐ High ☐ Medium ☐ Low	☐ Negative brand impact ☐ Possible loss of employee lives ☐ Possible loss of life by general public ☐ Public lawsuits ☐ Negative publicity
Product tampering—non-Company product but in associated category	☐ High ☐ Medium ☐ Low	☐ Negative brand impact ☐ Possible loss of life ☐ Slow business process recovery ☐ Public lawsuits ☐ Negative publicity
Theft and publication of customer lists with private data	☐ High ☐ Medium ☐ Low	☐ Negative brand impact ☐ Cost to protect customer privacy going forward ☐ Adverse litigation ☐ Regulatory sanctions
Loss of IT systems from malicious act	☐ High ☐ Medium ☐ Low	☐ Interruption to market share ☐ Major impact on manufacturing, sourcing, and sales ☐ Loss of investor confidence ☐ Major cost of alternate site and restoration of data

an integrated set of security elements keyed to the unique and likely threats previously identified;
the ability to train the dispersed safety or security assets to a level consistent with planned standards of incident response; and
the ability to *objectively* test all critical defenses and response capabilities and implement corrective actions.

3. *Execution*—This phase of the concept of operations relies on the tested competence of security assets you have established to respond to risk events:
the ability to lead as a risk event unfolds;
the ability to respond in such timely and effective ways that the risk event is mitigated with minimal loss or damage to corporate assets;
the ability to learn from the execution phase, to confirm what was anticipated, or to understand why contributing vulnerabilities were not previously identified; and
the ability to examine objectively plans, preparations, and response.

THE BOTTOM LINE: You have a broad and unique view of enterprise risk. Link that knowledge to the business alignment strategy, educate, and then take steps to ensure that your ability to respond is competent and prepared.

When there is an obligation to address resource reductions in response to adverse business conditions, use your knowledge to establish a threshold of risk tolerance, below which you no longer have confidence that the company is prepared to respond to what you believe has an increasing potential to occur.

Highlights for Follow-Up

- Understand the risks you own and those in which you share responsibility for some phase of management or elect to defer.
- Anticipate! Understand the potential source of the risk event(s) and how it would likely occur.
- Be aware of the impacts of emerging economic and strategic pressures on the business, and how developing corporate plans may impact the risks you should understand better than others in the management team.
- Advertise advice and requirements.
- Establish ownership for risk management and response.
- Offer assistance in installing and training on protection measures. Test their effectiveness frequently. Provide feedback on

results. Escalate if you don't see measurable improvement, then repeat the test.
- Establish key performance indicators appropriate to your programs.

Key Terms

- Risk assessment
- Risk mitigation
- Effective business controls
- Corporate liability
- Security program elements
- Response research
- Vulnerability assessment
- Risk quantification