ELSEVIER

Security Executive Council

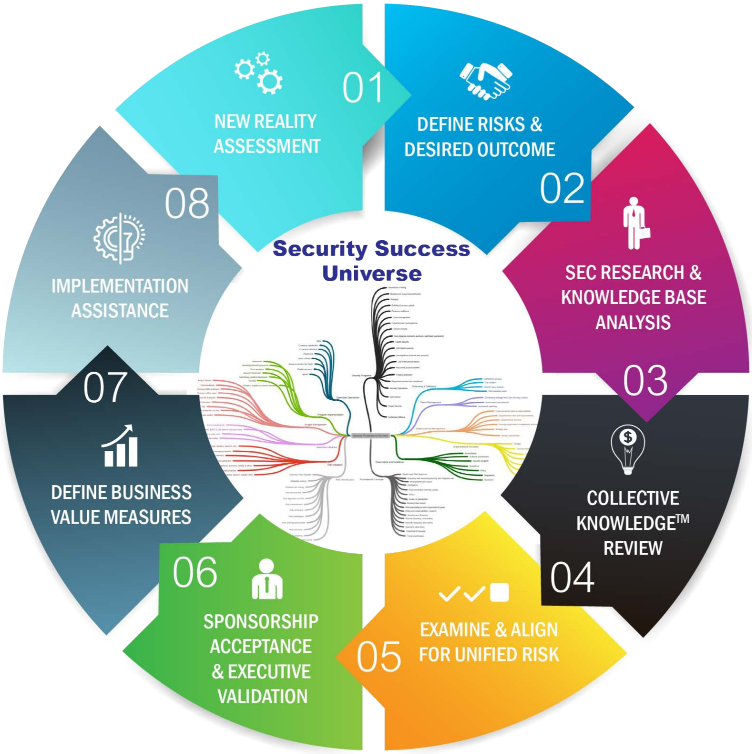
RISK MANAGEMENT PORTFOLIO

Influencing Enterprise Risk Mitigation

Francis J. D'Addario

THE SEC PROCESS

We walk clients through eight critical steps to reach their goals



01
NEW REALITY ASSESSMENT
DEFINE RISKS & DESIRED OUTCOME
02
SEC RESEARCH & KNOWLEDGE BASE ANALYSIS
03
COLLECTIVE KNOWLEDGE™ REVIEW
04
EXAMINE & ALIGN FOR UNIFIED RISK
05
06
SPONSORSHIP ACCEPTANCE & EXECUTIVE VALIDATION
07
DEFINE BUSINESS VALUE MEASURES
08
IMPLEMENTATION ASSISTANCE
Security Success Universe

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

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.

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

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

ISBN: 978-0-12-417233-3

CONTENTS

CHAPTER 2

The Geography of Risk

The relevance of local risk events and lessons learned ought to influence our scalable global protection. The Nisqually earthquake evacuated Starbucks world headquarters for weeks in February 2001. Other lessons came in September and October of that year. The experiences were instructive for the evolution of broader emergency preparedness and business continuity that enabled growth.

Local recognition and understanding of individual security requirements can inform prioritization of regional and global risk mitigation. Individual considerations and community needs may be addressed in the context of just-in-time preparedness. Mapping strategy to stakeholder needs stabilizes organizations and communities. Board level risk can thus be attended as key individuals and constituencies understand their roles.

To the casual observer, February 28, 2001 was an exceptionally promising Seattle winter day. Meteorologists were baffled: not a rain cloud was on the horizon and unseasonably mild temperatures were forecast. No specific security risks were on the radar that morning. The Starbucks Support Center tackled the normal protection requirements of a high-growth global coffee company.

Certain geologic forces were about to adjust the outlook. In a place called Nisqually, 57.5 kilometers SSW of Seattle, a 6.8 moment magnitude earthquake sprang from the depths, 52.4 kilometers below the docile surface. It shifted the seismic risk paradigm from a relatively remote regional occurrence in near geologic time to here and now in shockwave speed.

I was on the phone with Pete Rampp seeking assurance for the security equipment supply chain. My priorities changed mid-sentence as I was spun from my seat. The first force wave hit the nine-story square city block headquarters like a fully loaded freight train. I glanced at my clock as it swung on the wall. It was 10:55 a.m. Pacific Standard Time. Pete only heard my uncharacteristically abrupt, "I've got to go," and the tone of the dead connection.

The first concussion seemed to hit from the west as I sought safety in the crumbling office doorway. The hallway wall split and light fixtures blinked and crashed in the swell and roll. I found myself counting aloud

"31 one thousand, 32 one thousand" when a second force seemed to hit from the south. The north wall of the conference room disintegrated in a plaster dust cloud as the building banged against the adjacent parking structure.

That did it for me. At just under a minute with the building still convulsing I navigated the lurching fire escape stairwell three steps at a time for six floors. Inexperienced and untrained for seismic events, including "duck and cover," I relied on the fire evacuation orientation and exited at the front parking lot to witness the general evacuation; narrowly missing the brick and mortar that cascaded from above.

Within 30 minutes, more than 2,000 employees, service personnel, and visitors nervously awaited instructions in the parking lot. Cell phone service disappeared, sparking rumors of a regional disaster. Structural stability confirmation for bridges and buildings takes time to assess. I advised Rick Arthur, my boss, and Orin Smith, the CEO, that no serious physical injuries were yet reported.

Facilities immediately undertook the structural assessment of the building with the landlord and the city. Protection personnel surveyed the windows from all sides with binoculars, looking for people who may have had their escape obstructed as first responders were arriving. Information Technology brought up their plan for an orderly shutdown of the network. General re-entry was out of the question pending damage reports. The Partner and Asset Protection (P&AP) team made provisions for additional 24/7 security personnel to cover access control issues.

2.1 ASSESSING PRIORITIES AND THE STRATEGIC GAME PLAN

The building performed admirably during one of the state of Washington's largest seismic events. Foundational shock absorbers helped protect against serious structural damage. Swinging lights had severed fire suppression sprinkler heads, dousing the building in hundreds of tons of water. Within hours, senior leadership and designated critical personnel began mapping a building recovery process that would take months to clear water damage, replace fixtures, and advance the building to higher seismic standards.

Workarounds were required for networked critical processes including payroll, accounts payable, and automated retail ordering for stores. Supplemental processes were prioritized or innovated for recovery where existing plans fell short. The Starbucks Support Center suffered a great amount of non structural damage that could not be repaired for total re-occupancy until September.

Risk appreciation is a sobering phenomenon. The Nisqually earthquake was a relevant "near miss" event for Seattle. It allowed calculated appreciation for the mitigation previously accomplished and nimble management of support groups that could rise to the occasion when needed to deliver the promises of mission and values. It also fueled an expanded understanding that potential single points of failure could threaten the ability to recover. Nisqually also expedited larger considerations for comprehensive prevention, emergency preparedness, emergency management, and business continuity strategies. Risk reassessment and mitigation investment reprioritization are always required for continuous improvement.

Earthquakes are relatively predictable phenomena around the world within near geologic time. Seismologists and at least one computer model agree that a similar shift a bit closer to the city center could wreak considerably more devastation. A potential future Seattle fault line shift at a conservative force of 6.7 would likely kill 1,600 persons, injure 24,000, and displace 45,000 families. The epicenter of destruction would be uncomfortably close—damaging 10,000 commercial buildings and houses.[1] These implications drove business continuity and other risk mitigation investments for facilities, networks, and, most importantly, people, safety, and security.

The results of a more recent Society for Human Resource Management survey confirm that security and safety in the workplace are considered "important" or "very important" to their job satisfaction by nearly all workers (90%).[2] Similarly, Gallup research has shown that if there is a perception that leadership allows hazards to go unattended, employees will leave.[3] People who are afraid to be at work tend to feel underappreciated, uncared for, and underpaid. The combination of physical and economic safety concerns can impact loyalty, honesty, and the engagement required for customer service and product quality.

Following the earthquake evacuation, cross-functional recovery managers determined other dependencies in rapid order. Many left their purses, wallets, credit cards, checkbooks, personal identification, keys, and laptops in a building that was for all intents and purposes inaccessible. The stories of inconvenience and anguish ranged from an

[1] Daughton, "Pinpointing Devastation."
[2] Society for Human Resource Management (SHRM). "2012 Employee Job Satisfaction."
[3] Harter, Schmidt, and Keyes, "Well-Being in the Workplace."

inability to get home to impairments for banking, bill paying, and even grocery purchases. International travelers including consultants and visitors left behind tickets, itineraries, and passports. One unfortunate woman had abandoned her bridal gown.

Pressing asset transfers, contracts, research, lease agreements, and projects in progress were potentially at risk without a stout recovery effort. Retrieval of critical business items including passwords and personal belongings were prioritized. Requests for recovery were triaged by P&AP and expedited over weeks when access was limited to hard hat-equipped P&AP and facilities personnel.

It was later learned that during the quake a maintenance engineer had been changing bulbs for the Starbucks Siren icon. The Siren sits dramatically above First Avenue South, 12 stories above Starbucks Center, a crowned goddess enchanting every visitor and passerby with the alchemy of coffee. One can only imagine the poor fellow's ride atop that ladder. Her twisted steel frame evidenced the force that was conducted throughout the building.

Nearly all appreciated their luck. There were no critical injuries. On any other winter day an evacuation into a freezing rain could have suffered the consequences of exposure and hypothermia. Fortune also provided the recently vacated 25,000 square foot roasting plant five blocks away. It was still robustly connected to the existing network. An unsecured primary server tipped over by the rocking was set upright, rebooted, and operated as if nothing happened. Critical recovery operations were relatively unhindered by space or technology constraints.

The trauma of the event revisited some as traumatic events often do. More near misses could have had serious consequences. Many sensed the anxiety of re occurrence. More than a few expressed doubts about returning to the building. Counseling, open forums, and building tours addressed many fears. The company demonstrated that it cared. Continuous messaging and workarounds ensured uninterrupted payroll, store inventory distribution, and a prioritized recovery of the building. Communications kept affected personnel informed on a range of issues from personal property recovery requests to ongoing seismic risk. Counselors were brought in to advise and assist the traumatized.

Existing severe weather communication lines along with web sites, voice mail, and e-mail options were leveraged for relevant situation updates along with local market television messaging. A "tell, show, do" approach let the community know that all anxieties would be addressed. Rick Arthur, vice president of administration, and Orin Smith, the CEO, detailed building safety and refurbishing at open forums. Cross-functional teams stabilized the people tipping point through mitigation (see Figure 2.1).

Left to their own purposes people will take care of themselves and family first. Unengaged individuals may misinterpret that the organization is moving on without them if they don't know the plan. "Non critical" personnel may move on without informative communications, causing a talent loss that impairs long-term recovery, particularly if risk perception is unimproved. Leadership that anticipates and mitigates anxiety with thoughtful incremental messaging engages productive behavior by clarifying communication channels and reconnects separated individuals back to the community recovery plan.

Connecting the details of event mitigation back to the cultural priorities of people care, asset protection, and critical process recovery serves as a shock absorber to allow individuals to process their value to the community.

The dependencies on people for critical processes, from banking transactions to inventory management and payroll, were newly appreciated.

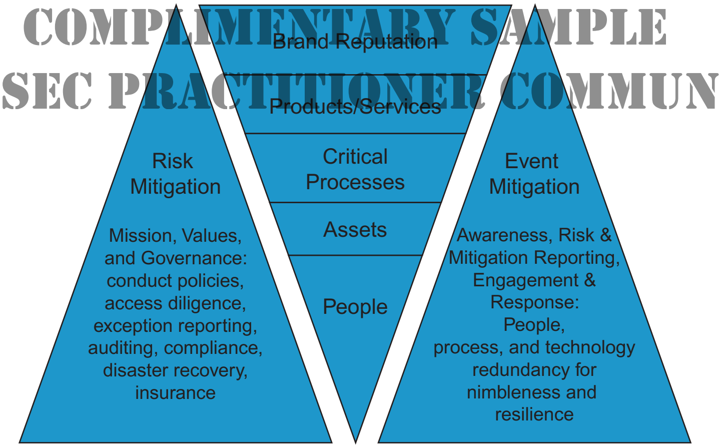

Brand Reputation
Products/Services
Critical Processes
Assets
People
Risk Mitigation
Mission, Values, and Governance: conduct policies, access diligence, exception reporting, auditing, compliance, disaster recovery, insurance
Event Mitigation
Awareness, Risk & Mitigation Reporting, Engagement & Response: People, process, and technology redundancy for nimbleness and resilience

Figure 2.1 Stabilizing the Tipping Point. © Crime Prevention Associates. All rights reserved. Used with permission.

Near single points of failure were added to the mitigation list for improvements. Key personnel were fatigued 72 hours after the quake. Service provider assistance mitigated potential burnout. Access control and premises security were passed to trusted service providers as building recovery operations were prioritized. Pre-positioning redundancy and services is a key consideration for business recovery and continuity of operations.

The Nisqually earthquake was a defining moment for many. Community morale and reputation were enhanced with every effort to care for people and make them feel safe again. Starbucks relied on its primary principle to provide a great work environment with respect and dignity. As with the triple murder in Washington, D.C., in 1997, honest conversations took place regarding ongoing risk and mitigation.

2.2 ALL-HAZARDS MITIGATION

Meeting and exceeding expectations for security and safety concerns can galvanize the community for greater investments. Starbucks was not content to merely reoccupy the building and restore processes to pre-event conditions. Leadership was determined to substantially improve both the facilities and risk mitigation capabilities. Emergency Response was evolving to Business Continuity as the result of cross-functional research and engagement.

Starbucks Center personnel and contractors welcomed the improvements that reaffirmed their choice of employment or assignment. Visitors seemed to appreciate a building orientation with emergency exit and seismic information that introduced many meetings along with a coffee tasting. Without mitigation, risk can wobble the foundation of the community, affecting people's confidence and ability to perform critical processes, produce quality product, deliver services, and maintain stakeholder confidence. Care, on the other hand, expresses values including commitment.

Innovation and teamwork accomplished process workarounds that guaranteed product to the stores. To the outside world, the effect of the Nisqually earthquake on Starbucks was a nonevent. Brand reputation survived intact because of good fortune and commitment to people. Inside Starbucks, the Nisqually quake shook additional realities into emergency preparedness. For instance, if the Seattle Fault line shifted with equal force, the needs would reach well beyond what the local public emergency first responders could provide. The 2,500 people in the headquarters parking lot could not be bystanders.

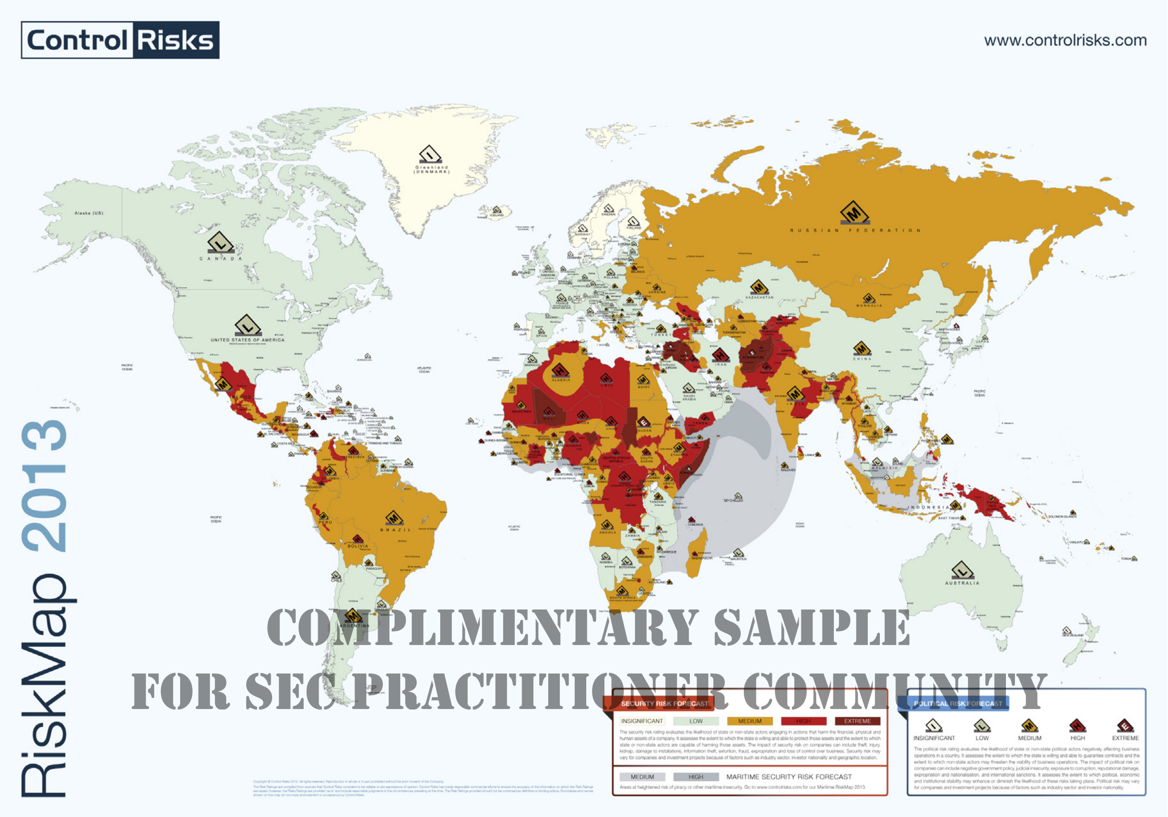
True emergency response and business recovery required a comprehensive plan and a cadre of self-actualized responders. Ideally, Community Emergency Response Team (CERT) trained and equipped personnel could provide for building evacuation, structural assessment, first aid, and search and rescue.[4] Scalable sustainability had to be developed with local capability worldwide. An expanding footprint promised more hazards. Although many had not yet imagined the likelihood of pervasive terrorism or pandemic prior to the 9/11 and "Amerithrax" attacks, the need to deal globally with both natural and manmade catastrophic events had become clear.[5]

Extended markets, supply chains, and networks require protection. Understanding global risk and mitigating it in a locally relevant fashion presumed a broader effort. Security and political risks are routinely forecasted by governments and private sector enterprises to inform constituencies from citizens to client organizations on the relative hazards of travel, business continuity, or expansion. Figure 2.2 is an example of a global security and political risks map developed by Control Risks, an independent global risks consultancy. It depicts hazards in color from insignificant (white) to low (pale green), medium (orange), high (red), and extreme (crimson).

Control Risks' ratings assess the likelihood of risk by calculating the impact of a wide range of factors including theft, injury to employees, kidnapping, damage to installations, information theft, fraud, extortion, expropriation of assets, and loss of control to an organization's assets in a particular country. Conditions may vary greatly between cities or provinces within the same region depending on local

[4] The Community Emergency Response Team (CERT) program is made available through FEMA (http://www.fema.gov/community-emergency-response-teams). Citizen Corps educates people about disaster preparedness and provides training for skills such as fire safety, light search and rescue, team organization, and disaster medical operations (http://www.ready.gov/citizen-corps). The *Are You Ready?* guide provides a step-by-step approach to disaster preparedness by informing readers about local emergency plans, how to identify hazards that affect their local area, and how to develop and maintain an emergency communications plan and disaster supplies kit (http://www.ready.gov/are-you-ready-guide).

[5] The FBI provides a detailed history of the anthrax attacks that began in the United States immediately following the 9/11 terrorist attacks: http://www.fbi.gov/about-us/history/famous-cases/anthrax-amerithrax. Five people were killed and 17 became sick when they opened pieces of mail that contained the deadly anthrax spores.



The security risk rating evaluates the likelihood of state or non-state actors engaging in actions that harm the financial, physical and human assets of a company. It assesses the extent to which the state is willing and able to protect those assets and the extent to which state or non-state actors are capable of harming those assets. The impact of security risk on companies can include theft, injury, kidnap, damage to installations, information theft, extortion, fraud, expropriation and loss of control over business. Security risk may vary for companies and investment projects because of factors such as industry sector, investor nationality and geographic location.

Areas at heightened risk of piracy or other maritime insecurity. Go to www.controlrisks.com for our Maritime RiskMap 2013.

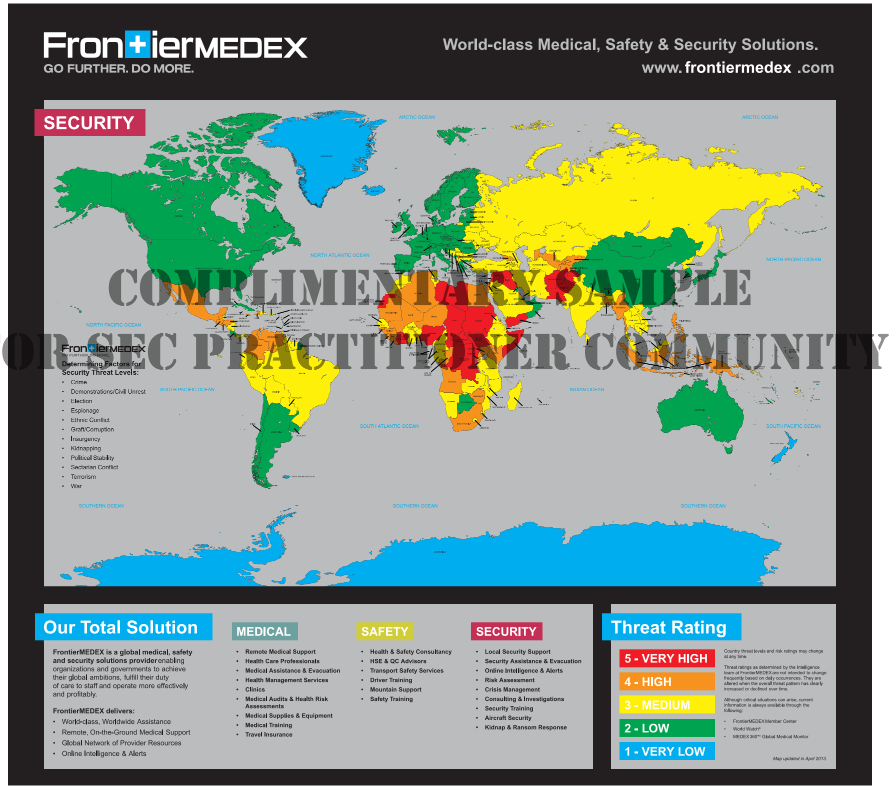
The political risk rating evaluates the likelihood of state or non-state political actors negatively affecting business operations in a country. It assesses the extent to which the state is willing and able to guarantee contracts and the extent to which non-state actors may threaten the viability of business operations. The impact of political risk on companies can include negative government policy, judicial insecurity, exposure to corruption, reputational damage, expropriation and nationalisation, and international sanctions. It assesses the extent to which political, economic and institutional stability may enhance or diminish the likelihood of these risks taking place. Political risk may vary for companies and investment projects because of factors such as industry sector and investor nationality.

Figure 2.2 Risk Map. © Control Risks Group Limited. All rights reserved. Used with permission.

situations. Organizations or institutions with global dependencies may require virtual risk information, including climate conditions if they are dependent on products from a certain region. Other risk probabilities for maritime security, such as piracy (shaded gray in Figure 2.2), must also be considered to design all-hazard risk mitigation.

Known terrorist operations shape the risk landscape and shade the mapping. Multinational terrorist operations continue to garner attention post 9/11. Coalition allies, including businesses and private citizens, remain targets for violence. Figure 2.3 is an illustration of known security threats patterns by country. Multinational terrorist operations continue to garner attention post-9/11. Coalition allies, including businesses and private citizens, remain targets for violence.

Orientation by maps and relevant data enables the student of global risk to understand the multidimensional nature of risk including the



Determining Factors for Security Threat Levels:

- Crime
- Demonstrations/Civil Unrest
- Election
- Espionage
- Ethnic Conflict
- Graft/Corruption
- Insurgency
- Kidnapping
- Political Stability
- Sectarian Conflict
- Terrorism
- War

Our Total Solution

FrontierMEDEX is a global medical, safety and security solutions provider enabling organizations and governments to achieve their global ambitions, fulfill their duty of care to staff and operate more effectively and profitably.

FrontierMEDEX delivers:

- World-class, Worldwide Assistance
- Remote, On-the-Ground Medical Support
- Global Network of Provider Resources
- Online Intelligence & Alerts

MEDICAL

- Remote Medical Support
- Health Care Professionals
- Medical Assistance & Evacuation
- Health Management Services
- Clinics
- Medical Audits & Health Risk Assessments
- Medical Supplies & Equipment
- Medical Training
- Travel Insurance

SAFETY

- Health & Safety Consultancy
- HSE & QC Advisors
- Transport Safety Services
- Driver Training
- Mountain Support
- Safety Training

SECURITY

- Local Security Support
- Security Assistance & Evacuation
- Online Intelligence & Alerts
- Risk Assessment
- Crisis Management
- Consulting & Investigations
- Security Training
- Aircraft Security
- Kidnap & Ransom Response

Country threat levels and risk ratings may change at any time.

Threat ratings as determined by the Intelligence team at FrontierMEDEX are not intended to change frequently based on daily occurrences. They are altered when the overall threat pattern has clearly increased or declined over time.

Although critical situations can arise, current information is always available through the following:

- FrontierMEDEX Member Center
- World Watch®
- MEDEX 360™ Global Medical Monitor

Map updated in April 2013.

Figure 2.3 Threat Map. © 2013 FrontierMEDEX Inc. All rights reserved. Used with permission.

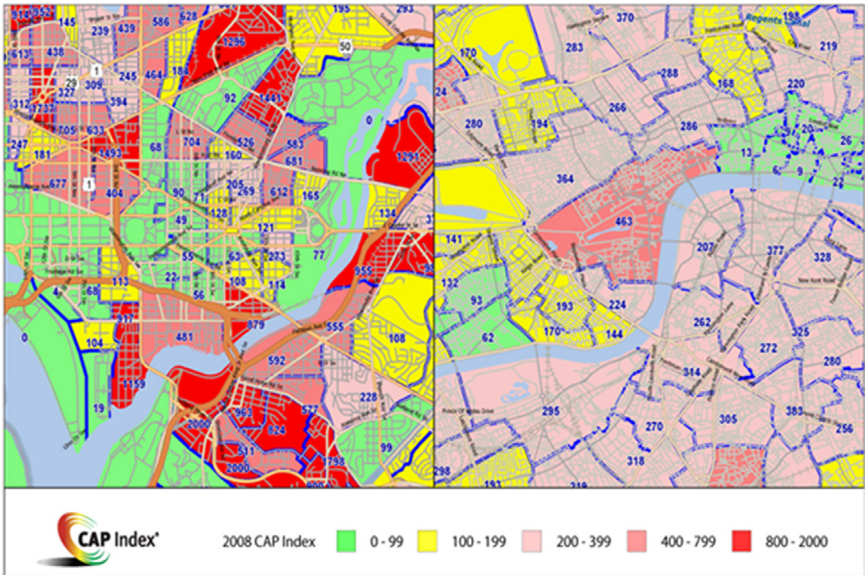


Figure 2.4 Washington DC and London Crime. © 2008 CAP Index. All rights reserved. Used with permission.

propensity for some hazards to traverse nominal political borders. Discrete information, including breaking news, can be detailed and imaged for catastrophic events, evolving threats, and environmental conditions to enable nimble preparation or response.

Local risk specificity is also easily depicted to highlight comparative data. Crime incidence is mapped in many parts of the world by responsible law enforcement organizations. Crime information, including sex offender data, is increasingly available to the public. In addition to municipal criminal incidence, indexed data is also available from private sector resources such as CAP Index for Canada, the United States, and the United Kingdom.[6] The CAP Index represents the risk of crime on a scale of 0 to 2,000 with 100 representing the average incidence for United States census track or United Kingdom ward population data (see Figure 2.4). Relative risk warrants a deeper dive for conditions and mitigation requirements when relevant hazards threaten community activity. Proprietary crime reporting offers

[6] Visit the CAP Index website to create customized crime reports of any address, neighborhood, or area in the United States, Canada, or United Kingdom: http://www.capindex.com/.

additional trend information that indicates actual crime experience. Broad implementation of robust security mitigation measures may guard against hazard conditions that change or travel from adjacent boundaries. Crime data instructs risk for local market hazards.

2.3 JUST-IN-TIME PREPAREDNESS

Post-9/11 and prior to the D.C. sniper and Tube bombing events that occurred in 2002 and 2005, respectively, Starbucks P&AP mapped “tier one” homeland security (high risk) cities, including Washington, D.C., and London, replete with coffee store locations, offices, and distribution points. This allowed calculation of risk adjacencies and business continuity contingencies for both events. Brand ubiquity requires nimble adaptation for global risk. Government and private sector intelligence can mitigate the same threats.

Unplanned events will also occur. Specific and incidental risk will vary. On September 11, 2001, many global and local organizations operated in the shadow of the World Trade Center or near the Pentagon. Adjacency to both Wall Street and the military, the professed specific targets of Al-Qaeda, put all in harm’s way.

Specific threats, adjacencies, and incidental risk may be anticipated. Knowing your neighbor’s risk and emergency plan may be beneficial, particularly when accidents or acts of sabotage have potentially devastating collateral effects. Adjacencies to atomic facilities or petrochemical processors may inform risk and mitigation planning differently than those for icons, mass transit hubs, or other infrastructure targets. Knowing risk mitigation particulars and incorporating them into your plan will potentially inform evacuation or shelter-in-place options.

Communities that care share risk information to enable their constituents. Those in need can sometimes galvanize news agencies, police, politicians, and local citizens groups to action. The birth of the World Wide Web and the resulting speed of communication aids preparedness and response. The web, along with other broadcast media including radio and television, may be leveraged for just-in-time awareness and mitigation. As an additional risk calculation, the web has also played a role in terror orchestration, as have other telecommunications networks. It may serve to bear in mind that all infrastructure

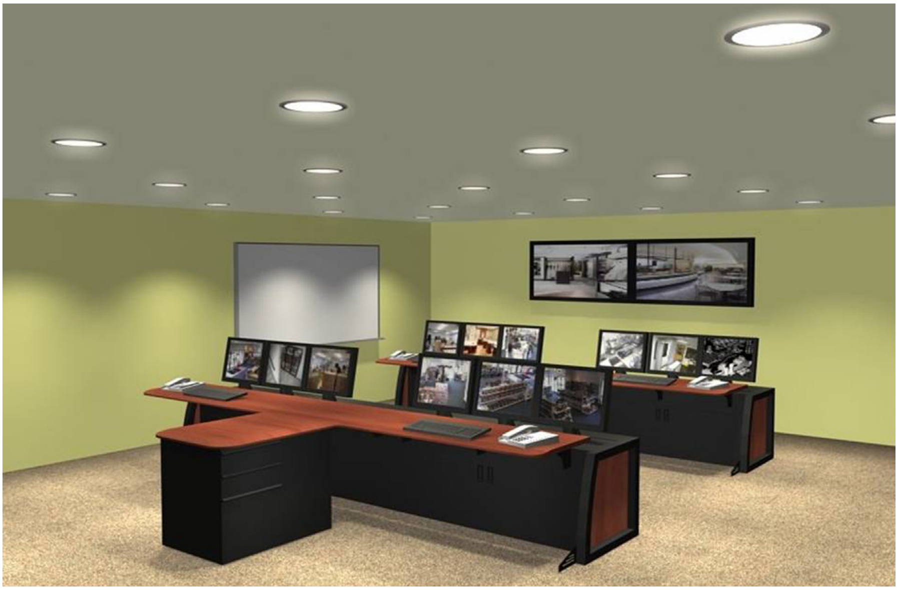


Figure 2.5 Security Operations Center. © Diebold, Inc. All rights reserved. Used with permission.

networks are subject to attack, compromise, or overload. Communications redundancy is recommended.

Ideally, mitigation information for known hazards should be shared prior to predictable emergencies. CERT training is one example. The concept of "Three days three ways" enables personnel and their families to anticipate the need for 72 hours worth of food, water, and emergency needs for home, work, and evacuation contingencies.[7]

Proliferation of post-incident information should occur on all available channels. It is often impaired by telecommunication network overload. Pre-event information dissemination and redundancies may hedge this shortfall. Security operations centers (SOCs) allow networked, redundant broadcast and Internet-enabled news and intelligence. An artist's rendition appears in Figure 2.5.

[7] "The 3 Days 3 Ways Disaster Preparedness Workbook," developed by the King County Office of Emergency Management and the American Red Cross, projects a very simple message to the residents of King County, Washington: be prepared to survive on your own for a minimum of three days following a disaster. For large disasters, government assistance may not be available for up to seven days. The three ways to become prepared include: making a plan, building a kit, and getting involved (http://www.xmarksthesound.org/pdfs/).

The concept depicted in figure 2.5 is a four-operator console with flat screens and an interactive whiteboard for project development or crisis management. SOCs may simultaneously connect to numerous peripheral platforms to follow evolving risk events, ensure access control, track travelers, and monitor security services. Single platform integration can offer value-added capability including enterprise-wide emergency status communications, alarm monitoring, virtual video surveillance or event corroboration, exception detection, and investigation development. The objective is to ascertain risk conditions for stakeholders, facilities, and their respective communities worldwide while deterring or impacting criminal activity and its related cost.

Subscription mapping software products can illustrate reported events within existing retail market, manufacturing, and supply chain coordinates with travel information. The idea is to globally discern, at a glance, all hazards for business operations, suppliers, networks, and travelers. Nimble risk appreciation allows reaction to prevailing and evolving conditions that affect people, product, and process. Facility access control and interactive security systems can confirm both video and audio emergency event conditions. Operators may ascertain adjacent critical events ranging from reported crimes of violence to ecological accidents or terror strikes in order to determine risk for employee, customer, guest, or other stakeholders.

Risk reporting information may be shared by networked communications, mail, wallet cards, or on pay envelopes that are delivered weekly or biweekly around the globe. Local police, fire, and ambulance notifications will likely supersede other reporting requirements that are imposed by operating policy.

As we will see in Chapter Seven, governance rules may address a “duty to report” injury, damage, theft and/or threats, or conditions that may risk injury, damage, or theft. E-mail, instant messaging, and other interactive reporting methodologies may support the social contracts or policies adopted by the community. Every communicated risk condition requires current reporting contacts and network addresses to leverage data distribution for awareness, response, program reporting metrics, and improvement.

Worst-case scenarios will potentially feature a failing utility grid, precluding recharging peripheral devices. Security methodology must inform the client community of risk and enable condition reporting. Effective protection is layered and integrated for both risk detection and response. Routine processes and communications contacts must be printed in anticipation of grid and digital network failures.

Integration of virtual event notification and communications allows key personnel to be advised globally of evolving risks with hazard-specific mitigation for prevailing weather, health, security, and safety conditions.[8] Integrated capabilities allow condition advisories before, during, and after a trip. Simple mitigations range from trip timing to postponement. Mobile communications allow awareness of spontaneous and evolving hazards. Providers like Dialogic (www.dialogic.com) and Send Word Now (www.sendwordnow) link emergency and non-emergency global communications for their clients. More complex traveler aid may range from safe haven advisories and medical referrals up to country evacuation and repatriation.

2.4 MAPPING STRATEGY TO STAKEHOLDER REQUIREMENTS

At Avon Products, Bob Littlejohn surveyed his leadership for "what kept them awake at night." The list included natural disasters, pandemics, terrorism, product extortion, corruption, workplace violence, information security, and the insider threat. These risks were further developed with supporting intelligence provided by the US State Department's Overseas Advisory Council (OSAC) and others. Organization-specific threat assessment and communication are the logical step after ascertaining the public sector view.

Littlejohn's pragmatic risk approach to the private sector was seasoned by his years in command at the New York City Police Department and the New York City Office of Emergency Management. Willard Rappleye chronicled Littlejohn's achievements as a volunteer leader for the International Security Manager's Association (ISMA) and as vice president for global security for Avon Products.[9] Bob is credited with early efforts to coordinate chief security officer risk communications between government and the private sector post-9/11.

[8] International SOS (www.internationalsos.com/) helps organizations ensure the health and security of their travelers and employees around the world.
[9] Rappleye Jr., "Thrust and Counterthrust."

Management increasingly recognizes the requirement for competent security leadership. William Parrett, CEO of Deloitte Touche Tohmatsu, asserts the value of security leadership: "Central to the creation and sustained development of a culture of risk management is the chief security officer." Parrett makes the case for setting the tone at the top. The community recognizes that leadership cares. Risk awareness and security mitigation are required disciplines for all. A sense of duty and the concept of the community "social contract" are essential.

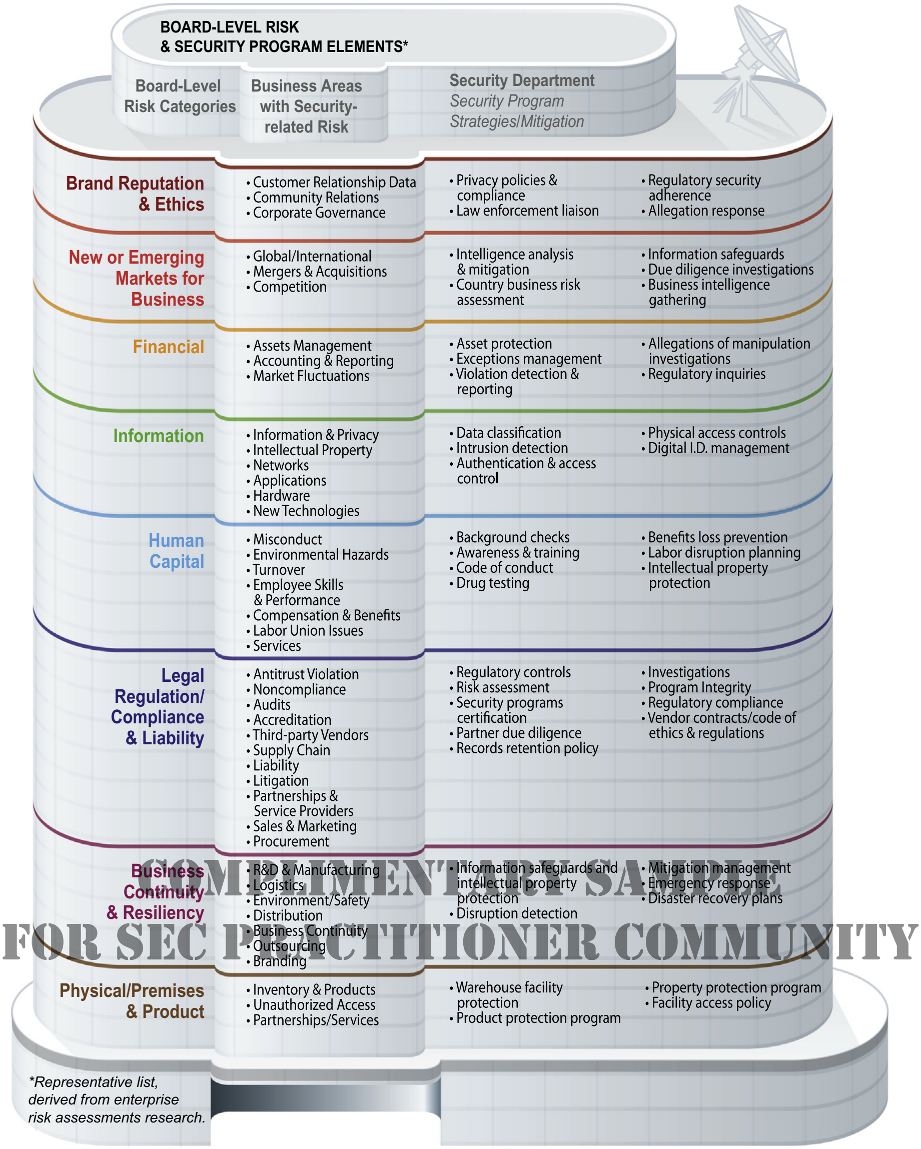
Parrett's underlying message to CEOs is that management, including boards of directors, cannot have a laissez faire attitude toward risk. The hazard landscape is too harrowing. The compliance environment after Enron and Sarbanes-Oxley requires more accountability. After the economic meltdown of 2008 and 2009, it will be more robust than ever. Current and evolving government requirements for emergency preparedness and business continuity will likely also hold leadership increasingly responsible for acts and omissions that fail to protect people and assets. To that end, the Security Executive Council, a problem-solving research and services organization, undertook the enumeration of board-level security risks (see Figure 2.6).[10] The hazards and security mitigation opportunities ought to interest stakeholders for any responsible organization.

As you can see in Figure 2.6, potential risks are numerous. Actual and vicarious experience within an industry segment or the public or private sector may inform your mindset. Failure to reasonably anticipate, prevent, or mitigate may introduce sanctions ranging from civil and criminal culpability to loss of insurance due to negligence.

Mapping risk relevant, breakthrough security goals and tactics three to five years out is a beneficial exercise for broadening security risk mitigation and ensuring resilience of new or maturing protection programs.

Our risk mitigation agendas will be longer than our careers. Connecting persuasively to the organization culture, strategy, and principal ambitions of the community is the key to our relevance and sustainability. Authenticating members of the community will likely be a

[10] Board-level risk is an industry-neutral research product, representing an amalgamation of diverse risk assessments.



BOARD-LEVEL RISK & SECURITY PROGRAM ELEMENTS*

Board-Level Risk Categories	Business Areas with Security-related Risk	Security Department *Security Program Strategies/Mitigation*	
Brand Reputation & Ethics	• Customer Relationship Data • Community Relations • Corporate Governance	• Privacy policies & compliance • Law enforcement liaison	• Regulatory security adherence • Allegation response
New or Emerging Markets for Business	• Global/International • Mergers & Acquisitions • Competition	• Intelligence analysis & mitigation • Country business risk assessment	• Information safeguards • Due diligence investigations • Business intelligence gathering
Financial	• Assets Management • Accounting & Reporting • Market Fluctuations	• Asset protection • Exceptions management • Violation detection & reporting	• Allegations of manipulation investigations • Regulatory inquiries
Information	• Information & Privacy • Intellectual Property • Networks • Applications • Hardware • New Technologies	• Data classification • Intrusion detection • Authentication & access control	• Physical access controls • Digital I.D. management
Human Capital	• Misconduct • Environmental Hazards • Turnover • Employee Skills & Performance • Compensation & Benefits • Labor Union Issues • Services	• Background checks • Awareness & training • Code of conduct • Drug testing	• Benefits loss prevention • Labor disruption planning • Intellectual property protection
Legal Regulation/ Compliance & Liability	• Antitrust Violation • Noncompliance • Audits • Accreditation • Third-party Vendors • Supply Chain • Liability • Litigation • Partnerships & Service Providers • Sales & Marketing • Procurement	• Regulatory controls • Risk assessment • Security programs certification • Partner due diligence • Records retention policy	• Investigations • Program Integrity • Regulatory compliance • Vendor contracts/code of ethics & regulations
Business Continuity & Resiliency	• R&D & Manufacturing • Logistics • Environment/Safety • Distribution • Business Continuity • Outsourcing • Branding	• Information safeguards and intellectual property protection • Disruption detection	• Mitigation management • Emergency response • Disaster recovery plans
Physical/Premises & Product	• Inventory & Products • Unauthorized Access • Partnerships/Services	• Warehouse facility protection • Product protection program	• Property protection program • Facility access policy

*Representative list, derived from enterprise risk assessments research.

Figure 2.6 Board-Level Security Risks. © The Security Executive Council. All rights reserved.

primary conditional requirement of the social contract prior to receiving its benefits and protection. The risk of counterfeit credentials and false identities to people, assets, and critical processes are consequential to every agenda.

Discussion Exercise

How do you make your clients aware of risk with relevant mitigation information? Have you developed a community emergency response team? Detail local and regional risks, resources, your plan, and a recommended survival kit for your community.

Additional Information and Resources

1. *Blindsided: A Manager's Guide to Catastrophic Incidents in the Workplace* by Bruce Blythe
2. IS 317: Introduction to Community Emergency Response Teams (CERT), an independent study course offered through FEMA's Emergency Management Institute, for those wanting to complete training or as a refresher for current team members (http://www.fema.gov/community-emergency-response-teams/training-materials).
3. "Preparing for the Unexpected," 5th edition, by the Commonwealth of Australia's Attorney-General's Department: http://www.em.gov.au.
4. Public Safety Canada: http://www.publicsafety.gc.ca/.
5. UK Cabinet Office's Emergency Response and Recovery Guidance: https://www.gov.uk/emergency-response-and-recovery.
6. "Disaster Preparedness for People with Disabilities," by the American Red Cross and FEMA: http://www.redcross.org/prepare/location/home-family/disabilities.
7. "Knowledge Corner: Business Continuity," the Security Executive Council: https://www.securityexecutivecouncil.com/knowledge/index.html?mlc = 603.
8. *Business Continuity Playbook*, edited by Dean Correia: http://store.elsevier.com/product.jsp?isbn = 9780124116481.

. . . the Nisqually quake experience prompted funding for a formal business continuity resource. It was put into action in 2005 when hundreds of stores and thousands of Starbucks employees were adversely affected before, during, and after Hurricane Katrina, the US Gulf Coast "storm of the century." Each was accounted for despite the complications of regional evacuations. What are known as "CUP" funds at Starbucks were designated for partner catastrophic assistance, and along with Social Responsibility's commitment of millions of dollars, the company enabled personal and regional recovery efforts.

China leadership was similarly guided during Starbucks' response to the catastrophic earthquake of May 2008. Reported deaths exceeded 69,000 with several hundred thousand injuries and millions of homes lost.

Like Katrina, all personnel were accounted for by the local crisis management team. Many suffered loss or injury of family members, homes, and untold emotional distress. In addition to assisting physical and emotional needs, substantial funding seeded contributions targeted for the recovery of schools.

ABOUT THE AUTHOR

Francis is a principal of Crime Prevention Associates and emeritus faculty of the Security Executive Council. He is a Certified Protection Professional (CPP), Certified Fraud Examiner (CFE), Community Emergency Responder, Food Defense Coordinator, and Coffee Master.

He is a seasoned all-hazards risk mitigation leader for multinational convenience, food and beverage, manufacturing, restaurant, retail, and supply chain operators. He has served as chief security officer for Starbucks Coffee, Hardees Food Systems, and Jerrico Inc. His expertise includes risk diligence, loss prevention, and mitigation systems design, as well as contribution analytics.

Francis was named one of the "25 Most Influential People in Security" in 2009 by *Security* magazine and was a *CSO* magazine 2007 Compass Award honoree.

He is also the critically acclaimed author of *The Manager's Violence Survival Guide* (1995) and *Loss Prevention through Crime Analysis* (1989).