DEPAUL BUSINESS LAW JOURNAL

SYMPOSIUM
"TERRORISM AND BUSINESS"

KEYNOTE ADDRESSES

ARTICLES

COMMENT

Volume 12 Fall/Spring 1999/2000 Numbers 1 & 2

RISK MANAGEMENT IN A DANGEROUS WORLD: PRACTICAL APPROACHES

Jonathan Tetzlaff

TABLE OF CONTENTS

Jonathan Tetzlaff has been involved with foreign affairs and international security analysis for over 20 years, working in a combination of government and corporate positions. Mr. Tetzlaff was hired by Congressional Research Service of The Library of Congress as a Foreign Affairs intern in 1979; he eventually spent 10 years at The Library, the last several as Senior Analyst, managing an interdisciplinary team of analysts. Mr. Tetzlaff was recruited in 1990 to become Amoco Corporation's first intelligence analyst, and was later promoted to Manager, Threat Analysis. In 1999, Mr. Tetzlaff was recruited by Merck & Co., to become Director, Security Systems and Programs, in the newly-created Global Security Group. His positions and comments are his own, and do not reflect the position of Merck & Co, Inc.

RISK MANAGEMENT IN A DANGEROUS WORLD: PRACTICAL APPROACHES

I. INTRODUCTION

Security incidents can erupt with startling suddenness virtually anywhere in the world, throwing even the most carefully crafted plans into turmoil. Many of these tragedies have an impact that ventures far beyond the victims themselves:

● On August 7, 1999, bombs exploded outside the U.S. Embassies in Tanzania and Kenya, killing more than 250 people, 12 of whom were U.S. citizens.[1] At least 5,000 were injured, the vast majority *outside* the targeted embassies. Victims included government employees, businesspersons working near the Embassies, and local residents.[2]

● On November 2, 1997, four Americans employed by Union Texas Petroleum ("UTP") were visiting Karachi, Pakistan, conducting an audit of local operations.[3] While driving from their hotel to the office, the auditors and their Pakistani driver were attacked by gunmen in an adjacent vehicle.[4] All occupants of the UTP vehicle were killed instantly by automatic-weapons fire; the assailants escaped.[5]

● On May 4, 1995, pipeline workers with the Bredero Price company were sleeping in company-arranged accommodations in the Algerian town of Ghardaia.[6] At midnight, 15 gunmen attacked

---

1. *International Manhunt Launched for US Embassy Bombing: FBI*, Agence France Presse, Sept. 18, 1998, *available in* LEXIS, Nexis Library, News Group File, All.

2. United States Department of State, *Report of the Accountability Review Boards on the Embassy Bombings in Nairobi and Dar es Salaam on August 7, 1998*, (visited Mar. 9, 2000) <http://www.state.gov/www/regions/africa/accountability_report.html>.

3. Steve Barth, *In Dangerous Places*, WORLD TRADE, Oct. 1998, at 64.

4. *Id*.

5. *Id*.

6. *French Survivor of Attack in Algeria Complains of Lack of Security*, AP Worldstream, May 9, 1995, *available in* LEXIS, Nexis Library, News Group File (on file with author).

the compound.[7] Armed with automatic weapons, bulletproof vests, and explosive devices, they killed five foreign workers: two Frenchmen, a Canadian, a Briton, and a Tunisian.[8] Four other foreigners survived the killing spree, which lasted at least 45 minutes, by hiding under beds or huddling precariously on outside windowsills.[9]

- On April 19, 1995, a bomb devastated the Alfred P. Murrah Federal Building in Oklahoma City, killing 168 people, including 19 children (most of whom were in the onsite daycare center).[10] Offices of a number of federal agencies were located in the building, including those of the Bureau of Alcohol, Tobacco, and Firearms.[11]

All four attacks were launched with little or no warning, and there were no known reasons to avoid the sites on the day of the attacks. Moreover, there have been numerous other terrorist attacks against government buildings, businesses, and individuals around the world. In view of these incidents, corporate management might understandably question whether a business can protect itself against such threats, when even governments – with their intelligence agencies, military support, and large security budgets – seem powerless to protect their own employees.

In fact, global enterprises can undertake a number of prudent steps to reduce, though not eliminate, risks.[12] Some precautions involve "traditional" solutions such as armored cars, bodyguards, and extensive physical barriers. In most cases, however, effective approaches to reducing risk are considerably more sophisticated, and involve a combination of risk analysis, pro-active risk management, and the employment of common-sense security precautions. This article outlines various approaches

---

7. *Id*.

8. David Ivanovich, *The Risky Business of Petroleum Politics; U.S. Oil and Gas Firms Must Often Weigh Instability in Some Areas with the Lure of Rich Reserves*, HOUS. CHRON., July 28, 1996, Bus. Sec. at 1.

9. *Id*.

10. *Oklahoma Bombing Haunts Survivors, Bystanders*, Deutsche Presse-Agentur, Aug. 15, 1997, *available in* LEXIS, Nexis Library, News Group File, All.

11. Joyce Peterson and Nolan Clay, *All Explosion Plotters Identified, Chief Says*, SAN DIEGO UNION-TRIB., Aug. 6, 1995, at A-12.

12. The scope of this document precludes consideration of many issues central to any comprehensive risk management program, including Information Security, Conflicts of Interest, Corruption, and Internal Investigations.

to risk management in a corporate environment, highlighting costs and benefits.

II. RISK CONCEPTS

Analyzing and managing risks is a complex endeavor. Risks and challenges to international business are highly varied: terrorism, crime, ethnic conflict, religious disputes, cultural differences, governmental corruption, challenging commercial environments, ill-defined legal systems, inadequate infrastructure, and a succession of changing political leaders are among the more difficult factors to assess and manage. Yet the true complexity of risk analysis is often much more fundamental, and involves an understanding of what *genuinely* imposes risk to a specific corporate endeavor or location.

Moreover, specific precautions to reduce risk may be counterproductive or yield unexpected outcomes. For example, some studies indicate that pedestrians suffer more accidents in crosswalks than when jaywalking because jaywalkers tend to exercise greater caution, and do not assume that a vehicle will avoid them.[13] According to the author Professor Gerald Wilde, there are numerous other examples in which precautions do not yield expected outcomes.[14]

---

13. GERALD J.S. WILDE, TARGET RISK -- DEALING WITH THE DANGER OF DEATH, DISEASE, AND DAMAGE IN EVERYDAY DECISIONS 91 (1994).

14. In the late 1960s, Sweden shifted from driving on the left side of the road (as in the United Kingdom) to the right side. Expecting numerous accidents in the first year, the government embarked on an ambitious public awareness program. In fact, at the end of the first year, *accidents fell substantially*, as increased education and driver caution offset unfamiliarity with the new driving patterns. Gerald J.S. Wilde, *The Theory of Risk Homeostasis: Implications for Safety and Health,* RISK ANALYSIS, 2, 209-225 (1982). In 1972, the Federal Drug Administration ordered child-proof caps on selected medicines. In 1984, one analysis concluded that 3,500 *additional* child poisonings had occurred annually because bottles were stored less safely and parents exercised reduced caution. W.K. Viscusi, *The Lulling Effect: The Impact of Child-Resistant Packaging on Aspirin and Analgesic Ingestions*, AM. ECON. REV., 74, 324-327 (May 1984). In 1986, part of a Munich, Germany taxi fleet was equipped with anti-lock brakes ("ABS"), and part was not. Drivers knew which vehicles had been altered. To the surprise of the observers, accident rates over a three-year period *increased* in ABS-equipped vehicles, as drivers drove faster, braked more abruptly, and cornered more sharply. Karl Michael Aschenbrenner and Bernhard Biehl, *Improved Safety Through Improved Technical Measures? Empirical Studies Regarding Risk*

Some observers interpret these results merely as proof of the well-known "law of unintended consequences." In fact, the situation may be somewhat more complex than that. According to the theory of *Risk Homeostasis*, people adapt their behavior in response to changes in their safety and security environment. In other words, human beings tend to "consume" changes in the safety and security environment, adapting their behavior in ways that keep their overall risk level essentially unaltered. Drivers with anti-lock brakes may brake more abruptly, bottles with "child-proof" caps may be stored less safely, and drivers faced with radically altered traffic patterns may reduce speed and increase caution.[15]

When dealing with the concept of risk (especially as it involves human behavior), therefore, it is essential to understand precisely which behaviors increase risks, and how best to reduce risks over the long term. Applying such an understanding to operations in higher-risk environments, such as Pakistan, South Africa, Mexico, Algeria, Colombia, Angola, and Nigeria, can yield important benefits, offering tantalizing glimpses that aid in shaping risk-management programs.

For instance, placing overseas staff (*expatriates*) in walled living compounds may actually increase risks, as frustrated expatriates may evade security precautions to "have some fun." Such evasion may appear low risk to the expatriates because as heavily protected employees, they become impervious to risks on a daily basis, and thus perceive little apparent danger. Similarly, excessive restrictions on travel to higher-risk locations may actually increase exposures. Infrequent travel reduces experience levels overall, increasing the likelihood of "simple" – and potentially deadly – mistakes.[16]

Infrequent travel also complicates development of effective *meet-and-assist* procedures; this author's experience has

---

Compensation Processes in Relation to Anti-Lock Braking Systems, in CHALLENGES TO ACCIDENT PREVENTION: THE ISSUE OF RISK COMPENSATION BEHAVIOR 81 (Rüdiger M. Trimpop & Gerald J.S. Wilde eds. 1994).

15. *See supra* note 15 for sources relating to these examples.

16. Infrequent travel (if it results in reduced oversight from corporate headquarters) can increase risks in other ways, also. Corporations headquartered in the United States are subject to the stringent guidelines of the Foreign Corrupt Practices Act of 1977 (FCPA), 22 C.F.R. §§ 709.1-709.8 (1999). In some locations, expectations with regard to FCPA-related activities are very different than in the U.S., and subsidiaries can unwittingly become involved in activities that may be common in the local operating environment yet illegal under the terms of the FCPA.

determined it be one of the more practical risk management tools for travelers to higher-risk locations.[17] *Meet-and-Assist* involves utilizing experienced "handling agents" who rendezvous with travelers at airports in challenging locations, guide them through customs and immigrations procedures, and place them on approved ground transportation to their local destination.[18] In locations where airport-based corruption is rampant, or taxi-based assaults common, this service can greatly reduce security incidents.[19]

III. RISK ANALYSIS

A. *Establishing a Sound Foundation*

1. Maintaining Analytical Independence

Analytical independence and integrity are essential elements of the "assessment" component of any risk management program.[20] Analytical independence can be difficult to ensure, as senior management can exert considerable pressure (often

---

17. Numerous sources outline a variety of meet-and-assist procedures, along with other related security precautions employed to manage risks. For one of the more useful summaries of corporate support to travelers and evacuees, *see* Eric Lassiter, *On Safer Ground; Bechtel's DeYoung on the Evacuation of Employees from the Persian Gulf*, TRAVEL WKLY., Apr. 29, at M11.

18. The need for meet-and-assist varies by traveler, and the sources of assistance are similarly varied. *See* Betsy Wade, *Practical Traveler; Getting Help At Airports*, N.Y. TIMES, Oct. 2, 1994, Sec. 5, at 4.

19. Such recommendations are common in the security industry and routinely employed by experienced businesses. One such recommendation, which focused on arrivals at Luanda, Angola's international airport is typical: "Only unregulated taxis are available at the airport. These should not be used: they are unsafe and present a high crime risk. Foreigners must be met by someone they recognise and who knows local conditions well. Carjacking is common on the road to the city centre. Security checkpoints along the route have been upgraded, but a small minority of police officers are corrupt and involved in armed robbery." Control Risks Group, *City Brief: Luanda, Angola*, Jan. 2000, at 1 (subscriber-only service available on the Internet <http://www.crg.com>).

20. For one of the more cogent descriptions of the "ideal" analyst, *see* LISA KRIZAN, JOINT MILITARY INTELLIGENCE COLLEGE, INTELLIGENCE ESSENTIALS FOR EVERYONE 55-60 (June 1999) (Part VII, *Portrait of an Intelligence Analyst*) [hereinafter KRIZAN].

unintentionally) in support of favored programs.[21] Moreover, analytical involvement in the early stages of program development – though offering distinct advantages in terms of shaping programs in a cost-effective manner – also has potential drawbacks. Analysts run the risk of being "captured" by the project team, becoming an enthusiastic proponent of the project rather than an evaluator of the process.[22]

Other pressures are also common, and can involve an employee attempting to downplay risks at one stage in the process and emphasize risks a short time later. In a particularly memorable case, an employee who expected to become Country Manager of a new operation, exerted considerable pressure on an analyst to downplay security risks. The prospective Country Manager was concerned that the analysis – which described a location with considerable security risk – might dissuade senior management from approving the project. The project was eventually approved, with a full understanding of the risks involved, and appropriate countermeasures were employed.

After approximately one year heading the new project, the Country Manager surprised the analyst by pressuring her to *emphasize* security risks, though they had not measurably changed. Discreet inquiries, prompted by this apparently contradictory behavior, revealed that a key component of the Country Manager's salary was essentially "danger pay." Once firmly established as Country Manager, he could increase his compensation by highlighting the dangers of living in that location.[23] In this

---

21. The former Chairman of the House Permanent Select Committee on Intelligence, Lee Hamilton, noted many years ago that "some of our recent intelligence failures may have occurred because key data and correct conclusions were washed away in a consensus-seeking process… Analysts must be free to speak up, to disagree and challenge…." *See* Lee H. Hamilton, *A Vigilant Congress is Key to Effective U.S. Intelligence*, L.A. TIMES, Mar. 10, 1985, Pt. IV, Opinion Sec., at 5.

22. *See* H. Bradford Westerfield, *Inside Ivory Bunkers, CIA Analysts Resist Managers' "Pandering"*, INT'L J. OF INTELLIGENCE & COUNTERINTELLIGENCE 407-424 (Winter 1996) (discussing of issues related to analytical independence and managerial pressure); *see also* H. Bradford Westerfield, *Inside Ivory Bunkers, CIA Analysts Resist Managers' "Pandering"*, INT'L J. OF INTELLIGENCE & COUNTERINTELLIGENCE 19-54 (Spring 1997).

23. The incident outlined in the preceding two paragraphs is based on the personal knowledge and experiences of the author during his tenure as a Risk Analyst.

situation, an alert analyst and supportive management avoided both attempts to manipulate the process.

2. Tailoring Data to Your Audience

Senior corporate management is deluged with information.[24] Internally-generated risk analysis must focus precisely on the needs of management, "adding value" by determining precisely the nature and type of information required. Though the requisite brevity of resulting reports can frustrate analysts, especially those with a strong academic background (who perceive the resulting product as simplistic or imprecise), longer documents are rarely read by busy senior corporate executives.[25] Corporate analytical documents, at least those that have an impact on decision-making, tend to be very succinct (perhaps a few pages in length), highly structured, and focused precisely on the locations and nature of the business in question.[26]

3. Identifying Reliable Source Materials

The risk assessment process requires accurate and timely data on key locations (especially remote, Third World locations) and events. Unfortunately, such data can often be difficult to acquire because of the remoteness of some locations, the fragmentary reporting on issues that are considered of little interest to a broader audience, and the inherent complexity of certain subjects (such as ethnicity and religious conflict).

---

24. *See* Clive Mathieson, *Cutting Through the Paper Mountain to Efficiency*, TIMES (London), Nov. 3, 1999, at 40 (discussing how the explosion of the Internet and e-commerce is forcing executives to rethink the archaic piles of "time-wasting paper documents" traditionally used to share information within an organization); and *Executives 'Growing Weary of Work Culture',* BELFAST TELEGRAPH, Oct. 26, 1999, *available in* LEXIS, Nexis Library, News Group File (on file with author).

25. One executive demands of his subordinates, "Don't tell me everything, just tell me what I need to know. If you try to know everything, you can't cope with it – it's too much." Jennifer Kingson Bloom, *Information Crush Shifting Execs into Overdrive*, AM. BANKER, Aug. 14, 1998, at A4.

26. One senior corporate executive has noted that the most successful committee that he ever chaired had a one-page limit on reports. *See* Declan Treacy, *Out with the In-Tray*, DIRECTOR, Jan. 1997, at 41 (stating "[i]t was hell getting people to adhere to that rule . . . [b]ut the great advantage of being brief was that people got to the nub of the problem.").

In many ways, the situation has improved measurably in the past decade, with such sources as CNN, Reuters, Radio France Internationale, British Broadcasting Corporation, and Sky News providing ever-more-rapid reporting of events worldwide. Yet such reporting is often inaccurate or incomplete.

Even when reporting is technically accurate, it can be misleading because media sources rarely focus on the specific corporation employing the analyst, or precise location in which corporate resources are based.[27] For instance, a terrorist incident in a remote location in Algeria may have little impact on corporate operations confined to the capital, Algiers. Yet media reporting will likely be non-specific, reporting a terrorist bombing "in Algiers" that, in fact, occurred 50 or 75 miles outside the city.

Of course, no "perfect" source exists. Governments can often provide a portion of the needed information. Usually reliable government sources include the UK Foreign and Commonwealth Office,[28] the US State Department,[29] and similar government sites.[30] As technology advances, such sources increasingly allow automated information gathering, sometimes through the creation

---

27. "It has been said that information from worldwide public sources constitutes some 90 percent of what policy makers needs to know, what is going on, and what will happen next, but that the missing 10 percent is critical." *See* WALTER LAQUEUR, A WORLD OF SECRETS: THE USES AND LIMITS OF INTELLIGENCE 91 (1985) [hereinafter LAQUEUR].

28. United Kingdom Foreign & Commonwealth Office, *Foreign & Commonwealth Office London (homepage)* (visited Mar. 9, 2000) <http://www.fco.gov.uk> (providing travel guidance).

29. United States State Department, *Travel Warnings & Consular Information Sheets*, (visited Mar. 9, 2000) <http://travel.state.gov/travel_warnings.html> (providing travel warnings from the U.S. Department of State).

30. Numerous other sites provide valuable information focused on specific needs. *See* Federal Aviation Administration, *Welcome to the FAA's Web Site (homepage)* (visited Mar. 3, 2000) <http://faa.gov> (providing guidance on air travel). Y2K-related travel information has been provided on countless sites in varied countries, *see* France Center for National Information, *Preparation for Y2K in France* (visited Mar. 9, 2000) <http://www.an2000.gouv.fr/> (France); United Kingdom, *Action 2000 – Millennium Bug* (visited Mar. 9, 2000) <http://www.bug2000.co.uk/index.html> (United Kingdom); and President's Council Information Coordination Center, *Welcome to the President's Council on Year 2000 Conversion Information Coordination Center (ICC) Monitoring the Year 2000 Rollover* (visited Mar. 9, 2000) <http://www.y2k.gov/> (United States).

of "personalized pages," in which the user selects the countries, regions, or topics of interest.[31] Other sites allow users to subscribe to automated electronic mailings tailored to individual interests.[32] Alone, however, government sources are insufficient to meet the needs of corporate risk analysts because they tend to focus on broad policy issues, not the concerns of specific interest to corporations. Other sources must be identified in order to provide the range of data needed for the effective functioning of the corporate risk analysis process.

Commercial sources can be critical to the success of a world-class risk analysis program. Such sources are varied, and include traditional media. However, an increasing variety of commercial risk analysis firms provide varied materials focused precisely on corporate needs.[33] These firms do not seek to advance the agenda or policies of any single government, and therefore offer somewhat more dispassionate analysis. One of the newer commercial sources is noteworthy in that it offers excellent and timely information tailored precisely to corporate needs. Provided by a risk consultancy headquartered in the United Kingdom – Control Risks Group – the source (*City Briefs*) provides "capsule" security guidance on approximately 350 of the world's largest cities.[34] Other commercial firms offer a range of source material;[35] the expertise of the individual firms tends to vary somewhat by region and topic, but overall quality of the major information providers tends to be good.

4. Coping with Risks and Limitations of Forecasting

In the view of many corporate and government decision-makers, an analyst's most important function is to forecast future

---

31. The U.K.'s Foreign and Commonwealth website offers particularly useful "personalization" features. *See supra* note 28. This site allows the user to create a user profile, providing information only on topics and countries of interest. *Id.*

32. The U.S. and U.K. sites both allow users to request receipt of automated electronic mailings on topics and countries of interest. *See supra* note 30.

33. Such firms include Control Risks Group, the Ackerman Group, Air Security International, Kroll O'Gara, TranSecur, and many others.

34. Control Risks Group, *City Briefs* (subscriber-only service available on the Internet <http://www.crg.com>).

35. *See supra* note 33 for a selected list of commercial firms.

events.[36] Regrettably, forecasting is one of the most unreliable and imprecise exercises undertaken by analysts. As British economist Norman Macrae observed, "[a]n extrapolation of the trends of the 1880s would show today's cities buried under horse manure."[37] Analysts seek to understand current structures and developments, thus aiding decision-makers in devising appropriate strategies. Venturing into the uncertain world of forecasting exposes analysts to countless variables and unknowns.[38] More importantly, analysts tend to "miss" some of the most important developments, because they are dramatic departures from the norm.[39]

Few acknowledged "experts" on Iran foresaw the rapid and total fall of the Shah, nor the crushing stranglehold that the Ayatollah Khomeini was able to exert upon the country.[40] This lack of foresight proved tragic for many, including the 52

---

36. *See* LAQUEUR, *supra* note 27, at 305-06. Laqueur states, "Intelligence analysts, like doctors, are expected to predict… Their customers wish to know not only what has happened but what is likely to occur in the future." *Id.* at 305. He further posits, "[t]hat forecasting underlies most human activities goes without saying; without some planning even the most primitive societies (based on hunting or agriculture) would not function… Yet the history of forecasting also show that knowledge of the past is by no means a sure key to the future." *Id.* at 306.

37. Anthony Paul, *Asia Needs a Green Revolution*, FORTUNE (Asia), Dec. 6, 1999, at 30.

38. According to Walter Laqueur, "it would be irresponsible for intelligence analysts to pretend to scientific accuracy in their forecasts about political and other developments. The unexpected death of a leader…may unbalance the equation so laboriously worked out… Seen from the decision maker's perspective, however, this caution may seem to be merely a manifestation of the bureaucratic impulse to avoid responsibility…." *See* LAQUEUR, *supra* note 27, at 141.

39. *See* KRIZAN, *supra* note 20, at 36 (outlining "Categories of Misperception and Bias"). The author defines *Evoked-Set Reasoning* as "[t]hat information and concern which dominates one's thinking based on past experience. One tends to uncritically relate new information to past or current dominant concerns." *Id.*

40. Bruce D. Berkowitz & Jeffrey T. Richelson, *The CIA Vindicated: The Soviet Collapse Was Predicted*, NAT'L INTEREST, Fall 1995, at 36. The authors conclude that "the intelligence community's failure to alert U.S. policymakers of the weakness of the Shah of Iran…occurred because the United States, in trying to maintain friendly relations with the Shah …failed to develop independent sources of information within Iran." *Id.* at 37.

Americans held hostage for more than a year.[41] Even more extraordinary, few analysts foresaw the rapid and total collapse of the Soviet Union, despite the massive intelligence and analytical resources focused on that country.[42] The concept was simply too extreme, too radical, to be accepted. Superiors, who found the forecast too unlikely to accept, too risky to advance, generally quieted the few analysts who sensed that dissolution of the Soviet Union was imminent.[43]

---

41. *See* Scott Macleod, *Can Iran be Forgiven?*, TIME, Aug. 3, 1998, at 44 (reviewing the assault by Iranian students on the American Embassy in Tehran, who held 52 Americans in captivity for 444 days).

42. Spirited debate continues over whether the Central Intelligence Agency foresaw the collapse of the Soviet Union. According to Richard Pipes: "Never has so much money been allocated to study one country; never have so many academic and government specialists scrutinized every aspect of a country's life. . . . Yet when the end came, the experts found themselves utterly unprepared." *Foreign Affairs* (Jan.-Feb. 1995) *cited in* Bruce D. Berkowitz & Jeffrey T. Richelson, *The CIA Vindicated: The Soviet Collapse Was Predicted*, NAT'L INTEREST, Fall 1995, at 36. Berkowitz and Richelson respond by asserting that "almost everyone…knows that the Central Intelligence Agency failed to anticipate the collapse of the Soviet Union. …There is only one small problem: The critics are wrong. …Throughout the 1980s, the intelligence community warned of the weakening Soviet economy, and, later, of the impending fall of Gorbachev and the breakup of the Soviet Union." *See* Berkowitz & Richelson, *supra* note 40, at 36.

43. Some experienced "Russia" analysts at the Library of Congress foresaw dramatic changes. In mid-1990, analysts at the Library's Federal Research Division correctly anticipated near-term Baltic independence and identified a series of factors that were to prove critical to the future of the Soviet Union. However, these analysts expected independence efforts of other Soviet states to be stalled for many years (perhaps even decades), and warned that widespread violence was likely. In fact, within 18 months, the Soviet Union ceased to exist, and the collapse (at least initially) was almost wholly without bloodshed. C. Migdalovitz and J. Tetzlaff, International Security Environment to the Year 2020: Global Trends Analysis (Apr. 16, 2000) (final paper presented at the Army Worldwide Long-Range Planners' Conference) (on file with author and Library of Congress).

B. *Conducting Effective Risk Analysis*

V. Analyzing Assailant Methodology and Target Selection

i. Nature

Understanding the *nature* of violent activity is an essential component of any risk analysis, yet a reliance on media reporting for information on terrorist incidents can be inaccurate or unhelpful.[44] Some "terrorism" may actually be common crime, yet is miscategorized by the media because it occurs in a location (such as Colombia or Algeria) where terrorism poses ongoing risks.[45] Other violence – or threats of violence – may be industry-specific, with very different groups targeting the oil industry, pharmaceutical firms, or airlines, for instance.[46] Assessing the threat to a specific corporation requires an understanding of these factors.

ii. Mechanisms and Goals

Another factor involves the *mechanisms and goals* of violence, specifically common crime, kidnapping, and terrorism. All may pose significant risks to corporate employees, but the nature of the risks (and therefore the appropriate countermeasures) vary considerably.

a. Common Crime

If local risks (even if considerable) primarily involve "common" crime, such as muggings or assaults, common-sense

---

44. *Media Coverage of Terrorism Criticized*, Associated Press, Sept. 22, 1986, *available in* LEXIS, Nexis Library, Wire Service File (on file with author). The article asserts that "Western news organizations contribute to worldwide terrorism by overreporting specific incidents and misreporting the overall nature of the world", and quotes Georgetown University senior fellow Michael Ledeen (himself a former reporter), "Most of the failures of the media come not from malice but from ignorance." *Id.*

45. Patrick Collins, Living in Troubled Lands 39-44 (1st ed. 1981) (providing guidance (and a checklist) outlining the importance of conducting a Threat Analysis, determining whether incidents are criminal or terrorist in nature, and understanding the nature of the targeting involved).

46. *Id.*

precautions appropriate to any large urban environment can often reduce risks to manageable levels.[47]

b. Kidnapping

Risk analysts must determine whether kidnapping occurs frequently in the location of interest. If so, assessing motivations is essential. Kidnappers motivated to a considerable extent by ideology may make demands that are very difficult (especially for a corporation) to meet, such as the release of jailed compatriots or changes in government policy. Kidnappers motivated primarily by profit may welcome straightforward negotiation to arrive at an acceptable ransom.

c. Terrorism

Some terrorists employ high-yield bombs, designed to destroy entire buildings (such as those utilized at the Khobar Towers attack in Saudi Arabia and the Murrah Building in Oklahoma City). To counter such risks, a thorough countermeasures program with a focus on perimeter security (including the selection of an office building set well back from the road) might be appropriate. If assassinations targeted at a single individual are a frequent method of attack, comprehensive route analysis and surveillance detection training, along with the utilization of armored vehicles, might be advisable.

If risk analysis indicates that terrorism poses significant exposures, assessing the nature of the terrorist act becomes essential. In other words, "one size does *not* fill all."[48]

---

47. One important crime overlaps categories: carjacking. The assault itself could be considered a "common" crime. The mechanism of attack, on the other hand, usually involves kidnapping (though the duration of detention can vary dramatically). The incident itself, as with any violent crime, is obviously terrifying and risks are considerable. Moreover, it can occur anywhere, not just traditionally higher-risk locations such as Pakistan or South Africa. For example, carjackings are a regular occurrence in major American cities. *See* U.S. Dep't of Justice, Office of Justice Programs, *Bureau of Justice Statistics Special Report, Carjackings in the United States, 1992-96* (visited Mar. 31, 2000) <http://www.ojp.usdoj.gov/bjs/pub/ascii/cus96.txt>.

48. *See infra* Part III.B.5 for additional consideration of these issues.

2. Understanding the Concept of "Soft Targets"

An understanding of the concept of "soft targets" is essential to risk management. A particular corporation may not be an assailant's primary target. In a terrorist's ideal world, an assailant with an anti-U.S. agenda may wish to kidnap a U.S. ambassador or bomb a U.S. Embassy.[49] As Western embassies continue to improve physical and personnel security, however, terrorists may shift to "softer" (i.e., more accessible) targets.[50]

In some cases, such soft targets may include high-profile U.S. businesses or their senior management.[51] For this reason, it is often advisable to maintain as low of a business profile as is practical, even in the absence of specific threats. Companies involved in oil exploration or production (rather than marketing) in a certain country may choose to minimize their physical presence, operating in low-profile buildings with few signs or other identifying characteristics. Pharmaceutical firms operating in countries where all prescription medication is sold to a national health management body may be able to adopt similarly discreet profiles. In both cases, key overseas operating locations may employ considerable security without unduly hampering business operations.

Companies that are primarily or exclusively retail in nature face particular challenges because the very nature of their business is one in which non-employees are actively encouraged to enter the premises.[52] For this reason, extensive physical security precautions may be inappropriate or impossible. The experiences of McDonald's (in Greece and France) and Kentucky Fried Chicken (in India) are prime examples of retail companies targeted by

---

49. Howard Levitin notes that "According to the U.S. State Department, as security for government buildings continues to improve, more businesses and public facilities are being targeted." *See* Howard Levitin, *Preparing for Terrorism: What Every Manager Needs to Know*, PUB. MGMT., Dec. 1998, at 4, 6.

50. Uzi Mahnaimi & Tom Rhodes, *Israel on Alert for Bin Laden Attack*, SUNDAY TIMES (London), Dec. 19, 1999, at 20.

51. *See* Levitin, *supra* note 49, at 5 (stating that "soft" targets are soft because of their "low risk for terrorism.").

52. Charles A. Sennewald, a security professional with extensive experience in the retail arena contends that "[a] retail security practitioner will be exposed to and involved in more crime, more arrests, and more investigations into loss in 2 years than his or her counterparts in other industries will experience in 10 years." *See generally* DAVID L. BERGER, INDUSTRIAL SECURITY (2d ed. 1999).

violence.[53] Restaurants of these and other firms have been picketed, attacked, and firebombed.[54] Such companies require highly specialized security programs, especially as they become the focus of intense nationalistic efforts to reduce competition and protect local products.

3. Preparing for Likely Risks

The risk assessment process requires a detailed consideration of *likely* risks, not necessarily *all* risks. The media and government, for instance, periodically warn of the risks posed by nuclear terrorism, bioterrorism, or other weapons of mass destruction.[55] Such risks are real, but expending enormous corporate resources to counter an assault with a weapon of mass destruction is rarely prudent or necessary. Such preparation, in the view of most corporate executives, properly falls within the province of government.[56]

---

53. *See* J.F. Burns, *Kentucky Fried Chicken on Front Lines in India*, INT'L HERALD TRIB., Sept. 15, 1995, Fin. Sec. at 20 (discussing KFC's troubles with Indian nationalists making an effort to "curb the entry of foreign corporations into [their] country."); *Terrorist Group Attacks McDonald's in Athens Suburb*, CNN, Oct. 4, 1999, *available in* LEXIS, Nexis Library, News Group File (on file with author).

54. *Leader of Farmers' Union Targeting McDonald's Freed from Jail*, CNN, Sept. 7, 1999, *available in* LEXIS, Nexis Library, News Group File (on file with author).

55. Author Jessica Stern notes that certain chemical and biological agents are readily available, and can be quite effective in certain circumstances. She perceives risks from nuclear terrorism as somewhat lower, in view of the challenge of building, deploying, and detonating a nuclear device. Stern speaks with considerable knowledge; while at the National Security Council, she ran the Nuclear Smuggling Interagency group as director for Russian, Ukrainian, and Eurasian Affairs. *See* JESSICA STERN, THE ULTIMATE TERRORISTS 1-4 (1999) (hypothesizing a terrorist attack with nuclear weapons on the Empire State Building in New York, and ultimately concluding that an attack using biological or chemical weapons would be easier to accomplish and could be just as deadly).

56. Howard Levitin notes that "[to] some, the perceived likelihood of a terrorist attack is so remote that planning for such an event is considered a poor use of limited resources." *See* Levitin, *supra* note 49, at 7.

Exposures related to cyberterrorism are also widely discussed by media and government sources.[57] Although such risks fall into a somewhat different category than bioterrorism or nuclear terrorism, the end-result could be devastating to a corporation. Cyberterrorism may pose genuine risks,[58] and most large corporations employ computer security professionals.[59] However, many knowledgeable observers believe that exposures are often exaggerated in the media. As a recent article in the respected *Jane's Intelligence Review* noted, "[c]yberterrorism is a buzzword of 1999. Indeed, with the remarkable growth of the Internet, hacking horror stories have reached new heights of publicity, leading to a veritable media frenzy. Yet careful examination of the issue reveals much of the threat to be unsubstantiated rumour and media exaggeration."[60]

In 1999, an extraordinary level of attention was focused on the end of the millennium, and the extent to which computer related failures (the *Y2K* problem) could compromise logistics and security around the world.[61] Some warned that perimeter security

---

57. Matt Hamblen, *Clinton Commits $1.46B to Fight Cyberterrorism,* (visited Mar. 9, 2000) <http://www.computerworld.com/home/news.nsf/all/9901251clinton>.

58. "Cyber issues are new and not well understood…. But the basic attack tools -- computer, modem, telephone and user-friendly hacker software -- are common across the spectrum and widely available." *See* The President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (visited Mar. 9, 2000) <http://www.info-sec.com/pccip/pccip2/report.pdf>.

59. Ira Winkler, *Ounce of Prevention: Allocating Adequate Resources to Security and Systems Administration is the First Step Toward Protecting the Enterprise in 2000*, INFO. SECURITY, Nov. 1999, at 48, *available in* LEXIS, Nexis Library, Information Security Magazine File (on file with author).

60. J.J. Ingles-le Nobel, *Cyberterrorism Hype*, JANE'S INTELLIGENCE REV., Dec. 1, 1999, *available in* LEXIS, Nexis Library, News Group File (on file with author).

61. Some sources were measured in tone, but others warned that virtual chaos could result. For instance: "In the Y2K scenario, the problem will be national and even worldwide in scope! So who will we call on for rescue if everyone else is in the same boat? If utilities, food and fuel deliveries, medical care, communications, and other vital services are in difficulty or down nationwide and worldwide, even for a short time, all of the people and organizations that we normally rely on for disaster assistance will be having the same problems that we are! So who will help the helpers?" *See generally* LIA MARIE DANKS, BUILDING YOUR ARK: YOUR PERSONAL SURVIVAL GUIDE TO THE YEAR 2000 (DAL Enterprises 1998).

devices could fail at midnight on December 31, 1999 or that terrorists would launch coordinated attacks at numerous sites around the world.[62] In many corporations, Y2K precautions greatly exceeded likely exposures, a fact which was widely acknowledged only after December 31st passed almost without incident.[63]

Carefully crafted countermeasures should facilitate efficient management of a wide range of risks. However, countermeasures must focus primarily on *likely* exposures, such as crime, which may gain less media coverage than terrorism but occur far more frequently. Practical, cost-effective contingency plans are essential to this process, regardless of the specific risk at hand. A comprehensive program will manage a wide range of exposures simultaneously, avoiding the need to create a separate program for highly unlikely contingencies. For example, responses to biological or nuclear terrorism might be addressed to some extent within the context of a broader plan designed to address problems such as natural disaster.

Identifying risks that require a customized contingency plan requires an understanding of past patterns of attacks, current threat levels, and future trends. Such an analysis is often site-specific, and could change measurably by business and location. Although fringe groups periodically target a range of companies (including oil companies, fast food restaurants, and pharmaceutical firms), the specific activists tend to vary by industry.

---

62. As the millennium approached, hundreds of articles addressed risks related to terrorism and Y2K. One of the more interesting focused on a report from the U.S. Senate, which speculated that "[t]he very effort to fix Y2K problems has left the nation's businesses and federal government wide open to a broad spectrum of international attacks on its computer systems." Robin Lloyd, *Senate Report: Nation at Risk of 2K-related Terrorism* (Sept. 22, 1999) <http://www.cnn.com/TECH/computing/9909/22/cyberterror.y2k.report.03/index.html>.

63. The debate over the usefulness of Y2K precautions is likely is outlive this analyst. Certainly, one can argue that December 31st passed without incident precisely *because* extensive precautions were implemented. In November 1999, President Bill Clinton noted that extensive government preparation had greatly reduced risks and correctly predicted that "I expect we will experience no major national breakdowns as a result of the Year 2000 date change." *Remarks by the President on Y2K upon Departure to York, Pennsylvania*, The White House, Office of the Press Secretary, Nov. 10, 1999. (available on the Internet <http://www.pub.whitehouse.gov/uri-res/I2R…:pdi://oma.eop.gov.us/ 1999/11/10/8.text.1>).

4. Anticipating the Psychological Impact of a Security Incident

With these factors in mind, a key element of the contingency planning process involves analysis of the psychological impact of an event within a specific corporation.[64] In other words, apart from the actual loss, risk managers must assess the likely impact on current and future operations of a specific incident. Impact can vary dramatically by location.[65]

For example, if five employees of a large Western multinational corporation are killed at a worksite by a lone gunman, the personal tragedy of the loss is generally unaffected by the location of the incident. The corporate impact of the loss, however, will vary dramatically by location. If the killing occurs in the United States or United Kingdom, for instance, the likelihood of a corporate withdrawal by a large Western company is extremely low. Management in either country would likely assess the incident, compensate families, improve security, and resume business operations.

If the same incident – five employees shot at their worksite by a lone gunman – occurred in Pakistan, Algeria, or Colombia, however, the outcome might be very different. Many Western corporations might conclude that the risks of operating in such challenging locations were simply too great, and that wholesale departure from the country is warranted. Such departures may or may not be justified; conclusions can only be made on a case-by-case basis. But they can have an enormous impact on the depth and breadth of international operations, and even on overall corporate profitability (should a company overreact by ceasing operations in promising locations).[66]

---

64. Even the psychological costs of *creating* a corporate counter-terrorism program can be considerable, if not managed properly. "[T]errorists or guerrillas do not have to stage an attack on the company to be successful. Their simple existence may cost the company dearly. If the living conditions are hard and dangerous, morale will be affected, job performance will suffer, and profitable operations may become impossible. A Draconian security program may cause unneeded problems, worsen morale, and inhibit profitable operations more than terrorists themselves." ANTHONY J. SCOTTI, EXECUTIVE SAFETY AND INTERNATIONAL TERRORISM 30 (1st ed. 1986).

65. For a particularly well-written guide to contingency planning in one of the world's most challenging locations, *see* Tara O'Connor, *Profiting from Overseas Opportunities; Contingency Planning in Africa*, SECURITY MGMT., June 1, 1999, at 87.

66. When employees are kidnapped, exposures can be similarly dramatic. Kidnappings in the US, as demonstrated in the abduction/death of Exxon

In other words, corporations are more likely to cease operations in locations that are not "core" to the business. A cost-benefit analysis would suggest that the risks of operating in a marginal location are unacceptably high.

Similarly, to extend the analogy, the impact of employee deaths may be dependent to some extent, on the cause of the incident. Victims of common crime are mourned, of course, but their deaths may receive little media attention and have minimal impact on the corporate decision-making process. Victims of terrorism, no matter how random and infrequent, are often publicized worldwide, and their loss can have a major impact on future corporate activities.[67]

For these reasons, the loss of a human life in a corporate setting can have dramatically varying impacts on the corporation as a whole, depending on where and how the death occurred. Corporate management, therefore, must prepare for – and respond to – such tragedies in very different ways.

5. Avoiding Fatalism

Some observers conclude that there is an inherent randomness to risk, and that precautions are therefore meaningless. In old war films, an oft-quoted line involved the inevitability of death if "a bullet has my name on it." An updated version concludes that "sometime you're the bug and sometimes you're the windshield."

Such fatalism is largely misplaced. On rare occasions, of course, violent events occur that are almost wholly unpredictable. For instance, there was no known reason to avoid the Alfred P.

---

executive Sidney Reso, obviously don't prompt American companies to cease operations in the U.S. A similar incident in certain higher-risk countries could, however, prompt many Western corporations to consider halting operations in those locations. *See* Robert Hanley, *Officials Say Body in Forest Is Sidney Reso*, N.Y. TIMES, June 29, 1992, at B1; Associated Press, *Exxon Chief's Death Came Soon After His Kidnapping; Abduction: Body of Firm's International President Is Found in Forest. Murder Charges Expected Against Couple*, L.A. TIMES, June 29, 1992, at A14.

67. One of the corporations recently victimized by terrorism is Union Texas Petroleum, which lost five employees to terrorists in Karachi, Pakistan. Lawsuits filed by family members of the victims led to years of litigation. Although the company eventually won the lawsuits, UTP was purchased the following year by Arco Corporation, and ceased to exist as a separate company. Ann de Rouffignac, *Ripe for Takeover, Union Texas Accepts Arco's $2.47-Billion Offer*, HOUS. BUS. J., May 8, 1998, at 5A.

Murrah Building in Oklahoma City on April 19, 1995. Yet 168 people died that day,[68] including 19 children, most of whom were in the building's onsite daycare center.[69] Being caught in the wrong place at the wrong time poses obvious (and, to some extent, unavoidable) risks to us all.

However, few events are totally random. Instead, location, profile, or activity shapes risks.[70] Certain countries tend to present a higher risk overall: many analysts highlight risks in South Africa, Algeria, Nigeria, Colombia, Angola, and Pakistan.[71] Mexico[72] (especially Mexico City in recent years) also poses risks, even to experienced travelers and expatriates. In such countries, an unusually high level of physical security, employee training, and travel limitations may be appropriate.

Similarly, certain buildings, cities, or neighborhoods may be at particularly high risk despite being in a relatively safe

---

68. *See* Deutsche Presse-Agentur, *supra* note 10.

69. The highest number of casualties occurred in the "waiting room" of the Social Security Office, located at the explosion's "ground zero" in the Murrah Building. The explosion occurred at 9:02am, shortly after parents had dropped their children at the building's daycare center, the America's Kids Child Development Center. Of the 21 children in the center at the time of the explosion, 15 were killed. Four other children, in various locations throughout the building, were also killed in the explosion. *See* Tamie Ross, *Day Care Honors Smallest Blast Victims*, THE OKLAHOMA PUBLISHING CO., July 16, 1995 (on file with author).

70. *See generally* JOHN Z. KEPLER, ET. AL., AMERICANS ABROAD: A HANDBOOK FOR LIVING AND WORKING OVERSEAS (Praeger Special Studies ed. 1983). Kepler and his co-authors offer practical guidelines for travelers of all nationalities, not just Americans. Under the heading "Security Abroad," key precautions are summarized, outlining ways in which behavior and other factors shape risk levels. *Id*. at 128-29.

71. Controls Risks Group currently considers a number of countries at "Extreme Risk" or "High Risk" including Afghanistan, Algeria, Angola, Colombia, the Democratic Republic of the Congo (formerly Zaire), Nigeria, Pakistan, Somalia, South Africa, and a number of others. Risks vary considerably by location *within* each country, of course: few countries – border to border – have precisely the same risk level. *See City Briefs, supra* note 34 for information on the Control Risks Group.

72. The British Foreign and Commonwealth Office and the U.S. State Department both warn of risks in Mexico, including Mexico City, focusing particularly on the risk of armed robbery and taxi-related violent crime. *See supra* notes 28 and 29.

country.[73] Virtually everyone knows that some urban neighborhoods have higher crime levels than others, and should generally be avoided.[74] Often less obvious are the risks related to specific buildings, often government buildings, as we learned in Oklahoma City. In many countries, sites closely associated with certain Western governments may be at heightened risk.[75]

IV. Risk Management

A. *Designing an Effective Program*

Creating an organization that effectively manages risk is challenging, and few do it successfully. Some corporations make the basic mistake of narrowly defining "risk" as "security risk" (primarily physical security) without considering their exposure from such factors as information loss, computer viruses, and

---

73. Assessing risks requires avoidance of common pitfalls. In less-sophisticated (often smaller) U.S. corporations, for example, an ignorance of Islam leads to misunderstandings and unfounded fears about operations in Islamic countries. At the other end of the spectrum, corporations based in Asia and parts of the Middle East, viewing media reports on crime in the U.S., can harbor exaggerated fears of travel to (or operations in) the U.S. *See generally* J. MILLER, GOD HAS NINETY-NINE NAMES: REPORTING FROM A MILITANT MIDDLE EAST (1st ed. 1996) (providing a superb overview debunking many Western misperceptions about Islam); DR. N. SANAD, THE THEORY OF CRIME AND CRIMINAL RESPONSIBILITY IN ISLAMIC LAW (1991); and SHAYKH F. HAERI, THE ELEMENTS OF ISLAM (1993).

74. Virtually no one disputes the fact that crime rates are higher in some neighborhoods than others. The cause and identifiers of such differences, however, are the subject of spirited debate. Benjamin Brooks Schreiber, *U. Chicago Researcher Finds Neighborhood Aesthetics, Crime Unrelated*, CHICAGO MAROON via U-Wire, Jan. 12, 2000, *available in* LEXIS, Nexis Library (on file with author); United Press International, *Neighborhood Appearance Deceptive*, Dec. 16, 1999, *available in* LEXIS, Nexis Library, UPI File.

75. The U.S. Embassies in Kenya and Tanzania are among the better-known examples of recently-targeted Western government sites. *See* Agence France Presse, *supra* note 1; U.S. Dep't of State, *supra* note 2.

fraud.[76] Other corporations fail to assess the full extent of their risk, especially in financial and legal terms.[77]

Corporations still following traditional models also tend to fragment security management, viewing security as essentially the effective utilization of "locks and lights."[78] Once that mindset is erroneously established, the management of security assets appears logically to fall at a low level, with site or plant management.[79] Management at this level is closest to the problem, and therefore positioned to understand day-to-day risks from theft, assault, or similar exposures.

However, important developments in the security field are leading to changes in perceptions and practices, including recruitment of more highly specialized staff, an increasing focus on risk management, a growing awareness of the need for centralized security incident reporting, and the creation of more flexible management structures.

1. Recruiting a Specialized Staff

A revolution in risk management has occurred in recent decades, as far greater numbers of the world's corporations have expanded internationally, necessitating a dramatically different approach to risk management.[80] Not too many years ago, corporate security directors at many large U.S. corporations were retired police officers with little international experience.[81] One recent

---

76. *Simple Information: Security Tactics You May Be Overlooking*, SECURITY DIRECTOR'S REP., Nov. 1999, *available in* LEXIS, Nexis Library, Security Director's Report File (on file with author).

77. Apart from the obvious physical risks, the legal exposure to corporations from terrorist activities can be considerable. Such risks are not new; litigation has quickly followed many significant terrorist events in recent decades. As noted more than 10 years ago: "If a corporation is considered negligent in protecting its personnel, it could find itself facing a liability lawsuit filed by the executive or their estates… Having a contingency plan to deal with a terrorist situation could help shield a company from litigation." M.A. Hofmann, *Terrorism is Threat to Companies Overseas*, BUS. INS., Oct. 9, 1989, at 52.

78. *Are You Investing Your Resources in Real or Imagined Threats?*, SECURITY DIRECTOR'S REP., July 1999, *available in* LEXIS, Nexis Library, Security Director's Report File (on file with author).

79. *Id.*

80. J.B. Treaster, *Gumshoes With White Collars; Deal Spotlights New Shrewdness in Detective Business*, N.Y. TIMES, Aug. 29, 1997, at D1.

81. *Id*.

article effectively summarized the problem with many "traditional" corporate security organizations. According to the author, many security managers:

> [C]ultivate an image that they only handle 'select' problems (as such, many are only associated with physical security, not 'people' security); (2) are reactive, not proactive; security is viewed as the department that responds to problems; (3) have an attitude problem; allow the stereotype of security professionals to go unchecked, failing to promote themselves as business partners and team players; (4) have failed to raise the bar for the security department and link themselves to the business functions of their companies.[82]

Risk management staff in successful corporations are increasingly international in experience and background, often have advanced academic degrees, speak at least one foreign language, routinely travel to foreign locations, and have lived in more than one country.[83] Increasingly, the risk management firms that provide consulting services to major corporations are mirroring that image.[84] A corporation's ideal senior security executive – with a combination of government and corporate

---

82. *Is Your Department Losing Out to Human Resources?*, SECURITY DIRECTOR'S REP., Dec. 1999, *available in* LEXIS, Nexis Library, Security Director's Report File (on file with author).

83. The author notes that "[t]he security profession has traditionally been dominated by persons with a law enforcement, investigative, or military intelligence background… . In the future …most management positions in the security industry will go to highly skilled business executives… . Security managers can expect their companies to enter markets in many countries around the world… . The security team must understand each culture and the risks associated with it…, provid[ing] employees with …details about the risks in various countries." Ira S. Somerson, *The Next Generation Security Professional*, SECURITY MGMT., Jan. 1995, at 26.

84. One major firm with a proactive focus is described as hiring "men and women with advanced degrees, board-room manners and dog-eared passports… . They do not carry guns or brag about flirting with death… . And they are supplying a service that barely existed not that long ago." *See* Treaster, *supra* note 80.

experience in the international arena – interacts easily, effectively, and frequently with senior management worldwide.[85]

The increasingly sophisticated staff employed in such progressive corporations is often a relatively small group. A state-of-the-art corporate security group, despite growing international responsibilities, generally employs 20 or fewer professionals, and some organizations are far smaller yet.[86] This shortfall is filled with a wider array of carefully selected contractors and consultants, employed on a short-term basis for their specific skill-sets.[87] Smaller corporate staffs also devote less attention to "low value" activities.[88]

2. Creating a Focus on Risk Management

Effective risk management requires the understanding and support of senior corporate management, as well as a centralized strategic focus.[89] Such support is critical, as the financial and organizational resources required for effective risk management can be considerable and smaller security organizations will need to

---

85. The author refers to a recent survey that "illuminates an image of security professionals in mid- to large-size corporations as increasingly adept at speaking the language of the boardroom and more often brought in as respected participants when business decisions are made." Sherry L. Harowitz, *Security's Positive Return; Role of Security Professionals within the Corporate Culture*, SECURITY MGMT., Oct. 1997, at 28.

86. *Latest Benchmarks: Security Department Staff Size,* SECURITY DIRECTOR'S REP., Sept. 1999, *available in* LEXIS, Nexis Library, Security Director's Report File (on file with author).

87. William C. Cunningham and John J. Strauchs, *Security Industry Trends*, SECURITY MGMT., Dec. 1992, at 26.

88. The definition of "low value" activity varies by corporation, but generally includes petty theft and similar security incidents in which no injuries have occurred, the monetary loss is minor, and the impact on the corporation as a whole is inconsequential. Such efforts fall within the province of "site security" – security guards provided by contract. Contract security guards tend to offer corporations enhanced flexibility and reduced expense. *See Are You Investing Your Resources in Real or Imagined Threats?, supra* note 78.

89. Robert M. Figlio and Ira S. Somerson, *Fighting Crime with Statistics and Loss Reporting; Corporate Security Management*, RISK MGMT., Nov. 1990, at 47.

rely on other departments to function successfully.[90] The changes in the corporate "thought process" at all levels (involving travel, investment, and crisis response) can also be significant, and are best implemented when the support of senior management has been expressly communicated throughout the corporation.[91]

A centralized strategic focus is essential to gaining and retaining the support of senior management.[92] A security function that is highly localized, operating in relative isolation with little established connection with other corporate elements (especially other security elements), is often ineffective and may be unduly expensive.[93] Also, costs of a highly decentralized security function are not readily apparent to senior management, as they are absorbed into the operating budgets of numerous diverse units.[94]

3. Centralizing Security Incident Reporting

The traditionally decentralized security structure has another, more serious drawback. In a highly decentralized organization, security exposures and incidents are rarely known to senior management, so neither risks nor countermeasures are apparent.[95] Operating subsidiaries have little incentive to report losses or exposures to senior management because local management may assume that corporate headquarters has little professional capacity to assist with security matters or even that the occurrence of security incidents at their site could reflect unfavorably on their management capabilities.[96]

---

90. Patricia M. Fernberg, *Securing Your Best Corporate Interests; Interview with Ford Aerospace Director Jerry Guibord*, MODERN OFFICE TECH., Apr. 1990, at 65.

91. *See* Figlio and Somerson, *supra* note 89.

92. *See* Fernberg, *supra* note 90.

93. This centralized structure facilitates routine reporting to management, particularly important as senior security executives increasingly report at the highest levels of the corporation. "The number of security departments reporting either directly to the head of the organization (10 percent) or to the executive level (73 percent) suggests that security departments are gaining ground in their fight to be respected members of the corporate inner circle." *See* Harowitz, *supra* note 85.

94. R.F. Hayton, *Why are Companies Losing the Fraud Fight?*, SECURITY MGMT., Sept. 1999, at 224.

95. *Id*.

96. "Without [a] reporting requirement, lower-level managers tend to avoid bringing incidents of fraud in their department to the attention of higher-ups. They view the discovery of fraud or malpractice…as a poor reflection on

For this reason, a centralized incident reporting system offers important advantages. Consistent reporting of incidents worldwide can assist in the protection of corporate assets (especially employees) by identifying locations and operations with disproportionate security problems. Resources can then be deployed to these areas, often from locations in which management is over-spending on security.[97]

Customizing traditional databases for security incident reporting is costly and time-consuming, making "off the shelf" software a more attractive option. Only a handful of such security software packages exist, but the best of these allow extensive customization to meet the needs of the specific business.[98]
The information gathered from utilizing such software "helps convince management to fund programs and helps the security department target those funds more effectively. In today's corporate environment, being able to justify expenditures and track results is essential."[99]

4. Building a Flexible Management Structure

Although centralized focus and systematic security incident reporting – guided by the corporation's senior security executive – are increasingly common in many large corporations, the reporting relationships of local security management continue to vary widely.[100] In many corporations worldwide, virtually all security personnel report to a Corporate Security Director. Although this structure allows the Director broad perspective and control, it can be inflexible and highly time-consuming if not managed effectively.[101]

Other corporations retain the largely outdated "silo" structure in which local security staff reports exclusively to site

---

their management capabilities and as potentially career limiting… . In such cases, the corporate board is left unaware of the extent and cost of fraud in the organization. Consequently, they may not see the need to devote appropriate time and effort to developing countermeasures." *Id*.

97. *See* Figlio, *supra* note 89.

98. Peter E. Ohlhausen and Ann Longmore-Etheridge, *Does Your Data Deliver? Security Management Software*, SECURITY MGMT., Nov. 1996, at 85.

99. *Id*.

100. Ongoing discussions and dialogue with Daniel J. Mulvenna, Leesburg Associates, an international management consulting firm (Dec. 1999-Jan. 2000) [hereinafter Mulvenna]. Mulvenna was formerly Director of Security, Amoco Corporation (now BP Amoco) from 1988-1998.

101. *Id*.

management.[102] In such corporations, the highly decentralized structure can hinder comprehensive security incident reporting, consistent security programs, and effective utilization of resources.

One knowledgeable source notes that corporations utilizing the silo model suffer "a lack of cooperation, 'turf battles,' divergent and uncoordinated security programs/plans, duplication of efforts, and the consumption of greater resources (including budgetary resources) than necessary."[103] One way in which progressive security managers can avoid such pitfalls involves the creation of a flexible hybrid, in which local/site security staff report on a "hard line" to operating management in a specific location or subsidiary, and have a clearly-defined "dotted line" relationship with the Corporate Security Director.[104] This allows continued day-to-day direction by local management, yet facilitates strategic guidance and review by the Director. This structure also allows the Director to report knowledgeably and comprehensively to senior management on the full range of worldwide security issues and concerns, ensuring that resources are invested prudently throughout the corporation.[105]

B. *Common Sense Precautions*

A comprehensive list of precautions is far beyond the scope of this article (and a full complement of countermeasures is beyond the budget of most corporations). Some of the most widely feared "dangers" – such as terrorists detonating nuclear devices – are extremely unlikely to occur for a variety of reasons.[106] Extensive

---

102. The "silo effect" is broadly recognized as a barrier to effective use of corporation resources. "[I]n management jargon, 'the silo effect' [refers to] operational areas [or] hierarchies within a larger hierarchy, lined up on the organizational chart like silos on the Plains. The boundaries separating one from the other--like the metal walls of a silo--complicate attempts to cooperate across departmental lines." Kevin Lumsdon, *Why Executive Teams Fail and What to Do*, HOSPITALS & HEALTH NETWORKS, Aug. 5, 1995, at 24.

103. *See* Mulvenna, *supra* note 100.

104. *Id.*

105. *Id.*

106. "Fortunately, there is likely to be a negative correlation between psychological motivation to commit extremely violent acts and the actual ability to do so. Schizophrenics and sociopaths, for example, may *want* to commit acts of mass destruction, but they are less likely than others to succeed. Schizophrenics, in particular, often have difficulty functioning in groups, and group effort would be necessary for large-scale dissemination of

preparation for extraordinarily unlikely events has limited utility, and consumes scarce resources better deployed on more likely scenarios.

Fortunately, a range of common-sense precautions has broad applicability in a variety of settings:

1. Analysis

Trusted and experienced individuals must be tasked to analyze specific sites, operations, and events. This analysis should not focus on risk levels overall; instead, the assessment should highlight likely exposures *to the corporation*, including employees and operations alike. Ongoing *re*assessment of risks is also important, as the absence of a disaster can be misinterpreted as an endorsement of the existing precautions.[107]

2. Contingency Planning/Crisis Management

Based on a thorough analysis, corporations should develop contingency plans for likely exposures. In certain (rare) cases, preparation is appropriate even for *unlikely* events, because of the specific manner in which these crises must be handled. A thorough *Kidnap and Extortion Response Program*, for example, is recommended for all large corporations. The document would specify responsibilities, key participants (including senior management, legal, public affairs, security, and pre-selected outside consultants), and a range of appropriate responses.

3. Travel/Operational Guidelines

Management must establish practical and reasonable travel and operational guidelines for key locations. These guidelines would specify travel restrictions (perhaps including requirements

---

chemical, biological, or radiological agents, or for producing a nuclear device." *See* Stern, *supra* note 55, at 77.

107. Dr. Richard Feynman, the Nobel Prize-winning physicist who assessed the Space Shuttle Challenger disaster as part of a Presidential Commission, concluded that "when the O-rings began to have problems and nothing happened, the agency began to believe that 'this risk is no longer so high' for subsequent flights and that NASA could 'lower our standards a little bit because we got away with it last time.' It is a kind of 'Russian roulette.'" Malcolm Gladwell, *Blowup*, THE NEW YORKER, Jan. 22, 1996, at 32-36.

for selecting or avoiding specific airlines[108] or locations), and outline other precautions to which adherence is required. In many locations, guidelines specify parts of cities to avoid.[109] Also, "route analysis" commonly specifies preferred roads and routing to specific locations, such as company headquarters or production facilities.[110]

4. Physical Precautions

Appropriate physical precautions (fences, lights, guards, weapons, armored vehicles, etc.) vary widely by location. Some corporations imprudently seek to impose a "corporate standard" worldwide under the mistaken assumption that consistency somehow offsets the need for site-specific countermeasures.[111]

---

108. Airline risk levels are difficult to determine, because of the relative infrequency of accidents and terrorist incidents per mile flown. However, broad guidance is possible, especially for airlines with particularly poor security or maintenance records. Travelers must also understand that airlines with the best security (El Al, for instance) may nevertheless have the highest risks, because of their attractiveness as a target to certain groups of terrorists.

109. The author outlines a series of guidelines optimized to reduce risks. Guidelines focus not only on locations to avoid, but also a series of general threat indicators, local threat indicators, vulnerability detection techniques, and methods to reduce and manage risks. KARL A. SEGER, PH.D., THE ANTI-TERRORISM HANDBOOK: A PRACTICAL GUIDE TO COUNTERACTION PLANNING AND OPERATIONS FOR INDIVIDUALS, BUSINESSES, AND GOVERNMENT, 77-101 (1st ed. 1990).

110. Collins, *supra* note 45, at 81-104. In this section, Collins provides extensive guidance on route analysis, surveillance detection, and travel security.

111. One large commercial bank took an innovative approach to managing the inherent tension between the need for consistent standards with the equally important requirement that countermeasures be optimized for the local environment. Barnett Banks "knew that it could no longer live with the inefficiencies that had become inherent in its decentralized approach to business" and "created… standardized security policies and procedures for the entire company." Concurrently, however, management instituted a security incident reporting system, allowing rapid modifications and enhancements to meet site-specific needs. Thomas Slimick, *One Bank's View of Security: Barnett Banks*, SECURITY MGMT., Feb. 1997, at 38.

5. Enforcement Mechanisms

A balanced and widely understood enforcement mechanism is essential, especially in higher-risk locations. Employees in locations such as Algeria, Nigeria, Pakistan, Colombia, and South Africa must understand that ill-advised actions (for example, ignoring travel restrictions) will not be tolerated, as they could place the company's entire operation at risk. The mechanism of enforcement does not require extensive discussion; instead, the corporation should issue a clear and concise policy regarding acceptable behavior.[112]

6. After-Action Assessments

Many corporations conduct structured "After-Action Assessments" following the conclusion of extraordinary events, including kidnaps, hijackings, emergency evacuations, or natural disasters. Operational efficiency of the emergency response mechanism is examined – highlighting successes and failures – and participants seek to identify ways in which future emergency responses could be improved.[113]

---

112. "The…policy statement…should define that there will be sanctions if corporate security procedures are violated. That's all the policy needs to say. Then you cascade that to the operating procedures for the individual profit centers. Involving your managers, not your security people, you should have an operating directive that defines those sanctions… . Some rules have to be laid down with some enforcement, with the stage set by corporate policy and implemented by the operations managers, not by the security manager." *See* Fernberg, s*upra* note 90 (quoting Ford Aerospace Director Jerry Guibord).

113. In many cases, no single critical error is responsible for a disaster. In her analysis of the Challenger Space Shuttle Explosion, Diane Vaughan writes: "The…Challenger launch is a story of how people who worked together developed patterns that blinded them to the consequences of their actions…. No fundamental decision was made at NASA to do evil; rather, a series of seemingly harmless decisions were made that incrementally moved the space agency toward a catastrophic outcome." *See* D. Vaughan, THE CHALLENGER LAUNCH DECISION: RISKY TECHNOLOGY, CULTURE, AND DEVIANCE AT NASA 410-11 (Univ. of Chicago Press 1996).

V. CONCLUSION

Corporations cannot prepare for every risk, every eventuality. Risk management has many components, many facets, only a few of which are covered in this article. Managing risks in a cost-constrained environment requires a measured and thoughtful analysis of likely exposures and practical, cost-effective countermeasures. Management and employees alike must realize that risks can never be eliminated; instead, an effective program is one that reduces risks to the greatest possible extent. As one thoughtful observer notes, "the safest among us are probably those who accept some level of risk, then keep an alert respect for danger – which is, after all, always present."[114]

114. John Lienhard, *Engines of Our Ingenuity, Acceptable Risk* (KUHF-FM radio broadcast No. 1097) (transcript available on the Internet <http://www.uh.edu/engines/epi1097.htm>).