2003

How to Handle the Threat of Catastrophe

Carol M. Sanchez
Grand Valley State University, sanchezc@gvsu.edu

Stephen R. Goldberg
Grand Valley State University, goldbers@gvsu.edu

How to handle the threat of catastrophe

Carol Sánchez and Stephen R. Goldberg
JCAF, 2003

One of the principal jobs of chief executives is to minimize risk and vulnerability to catastrophic events. Analyzing risk has become more complex since September 11, 2001. In addition to terrorism, other catastrophes can change the course of life as we know it including cyber crime, biological attacks, and the spread of diseases such as SARS. Companies must realign corporate priorities and put the security issue at the forefront, as many companies have done since the 9/11 attacks.

Risk management has dealt traditionally with two types of events: known risk and unknown risk. Known risks are events you know exist, and are somewhat likely to occur, such as fire, theft, accidents, lawsuits, economic or currency risk. Unknown risks are those that could happen, but are unlikely to affect you, your people or your property: earthquakes, tornados and other weather risks, political instability, and conventional terrorism, such as that to which the US was exposed prior to 9/11. We now have a third category: unknowable risk. Unknowable risks are those that are neither known nor unknown, and you don't imagine they exist. Therefore, it is difficult to plan contingencies for unknowable risks. Examples of unknowable risk include SARS, or passenger aircraft being flown into Manhattan skyscrapers.

Modern security threats: Terrorism

Companies are on the front lines in the war against domestic insecurity, because the main targets of terrorism include not just the U.S. government, but American infrastructure, icons such as the World Trade Center, major corporate brands, and

multi-national corporations[1]. While the U.S. government plans to spend over $60 billion on antiterrorist strategies in 2003, the U.S. private sector will probably spend twice that, up to $150 billion, on domestic security.

Companies will spend on traditional security items such as increased insurance coverage, physical plant security, security in operations and logistics, and information system protection, and new items including security vulnerability assessments, employee training in security measures, and perhaps appointing a security officer at the executive level [2]. The government is keen on creating security alliances with business, such as coordinating with financial service companies to verify truth of customer identity, supporting entrepreneurs who are developing new technologies with security potential and offering tax incentives to companies that invest in new security systems [3].

Modern Security Threats: SARS

In response to the outbreak of severe acute respiratory syndrome (SARS), the World Health Organization and the Center for Disease Control issued health advisory warnings against travel to affected areas (China, Hong Kong, Singapore, and Hanoi, Vietnam). Concern about SARS has affected the way companies do business with suppliers, third-party manufacturers and company owned operations in affected areas. To protect employees and the company, management has banned nonessential travel to these areas, and is looking for alternative ways to conduct business. Many solutions such as

[1] Marren, P.B. (2002, July-August). Business in the age of terrorism. Journal of Business Strategy, 19-23.

[2] Rothkopf, D.J. (2002, May-June). Business versus terror. Foreign Policy, 56-64.

[3] Varon, E. (2002, January 15). Homeland defense new rules of war. CIO, 40-44.

videoconferencing and communicating through computer-aided design software will permanently change ways of doing business.

The list of companies reacting to the epidemic is long. Motorola severely restricted travel to the area. Honda evacuated families of Japanese employees considered to be at risk. Gap stopped sending quality assurance teams to its contract manufacturers in Asia. Since over 50% of silicon chips and 85% of personal computers are assembled in Asia, Aberdeen, a Boston based IT consulting firm, advises original equipment manufacturers to have alternative sources of supply.

Industries that rely on face-to-face selling, such as financial services, are also suffering because of self-imposed travel restrictions. SARS has affected airlines, hotels, and conferences for virtually all businesses in the affected region. In past years, the Canton Trade Fair in Guangzhou has been the most significant export fair in China. This year, it was held in April, the original epicenter of SARS, and was effectively dead before it started.

Crisis Management Goals

The real threat of organizational catastrophe requires that management develop strategies and tactics to assure the safety and security for all company stakeholders – customers, employees, shareholders and the public at large – while successfully conducting business. Exhibit 1 identifies the three crisis management goals.

Exhibit 1
Crisis Management Goals

- Keep employees safe.
- Conduct business as usual.
- Provide extraordinary service in the wake of catastrophe.

Employee Safety

Employees at the company's physical locations should feel safe, and know that the company has a plan in case of an attack. Companies may stage simulated emergencies to practice building evacuation. One company in a high-rise location conducts safety drills once a quarter and has reduced the exit time from 25 to 14 minutes. Many firms are screening inventory and personnel more carefully, installing electronic employee ID systems, issuing magnetic cards to employees with emergency phone numbers and procedures, and putting fluorescent slip-proof paint on the stairwells. Others have restricted employee travel to essential-only.

Most companies want business to continue as usual or experience only minor interruptions if there is a catastrophe, preferring not to revert to backup plans or send employees home. This means that an organization-wide security strategy is a priority.

It is important to continue to provide extraordinary customer service if the nature of the business is critical to the reestablishment of public confidence after a catastrophe occurs. Many organizations in Manhattan did this immediately after the 9/11 attacks when New Yorkers were desperate for emergency health care, communications, financial and insurance services [4]. Within hours of the attack, technology companies such as Dell, HP, IBM and Sun set up emergency response centers. They hired additional call handlers to deal with the massive volume of emergency communication. Verizon created a virtual communications hub so Manhattan residents could access their email, voice mail and

[4] Craig, S. & Beckett, P. (2003, February 27). What will Wall Street do on red alert? Wall Street Journal, C1.

faxes. Many Manhattan banks forgave late payments and covered payrolls and overdrafts for some of their organizational customers. Northwest Mutual Life did not wait for beneficiaries to call before they started processing life insurance claims. They obtained flight manifests and employee lists, and processed nearly 160 life insurance claims in five days, rather than the usual 30 [5].

Security Planning

Exhibit 2 indicates the security strategies that should be highest priority in this environment of heightened risk.

Exhibit 2
Security Strategies

- Security planning: Overall and contingency planning for catastrophes.
- Physical security: Protection of physical premises.
- Cyber security: Protection of servers, software, and data.
- Asset security: Protection of company's assets.

Security Planning

A company's first priority is to make security a strategic function. Many large companies have created the new position of Chief Security Officer, thus promoting the security function from the basement to the executive floor. Sixty-three percent of firms surveyed by the Business Roundtable reported they have a chief of security [6]. Appointing a CSO at the executive level to the security function is the most aggressive way a company can assure that the security issue is part of its strategy. The CSO provides constant attention to risk, by keeping continuous contact with other company executives

[5] Gandossy, R. (2003, January-February). The need for speed. Journal of Business Strategy, 29-33.
[6] Fannin, R. (2003, January-February). Danger abroad. Chief Executive, 30-35.

to assess and protect security needs, and by networking with other CSOs for best practices.

Smaller, mid-market company executives may choose to hire security consultants instead of creating the CSO function. CEOs of these companies should seek professional advice to secure their computer networks, create business evacuation and continuity plans, and advice on the location of a back-up headquarters for physical and cyber operations. Exhibit 3 identifies critical steps that top management should take in its security planning.

Exhibit 3
Security Planning

1. Find your security strengths and weaknesses.
2. Reduce or eliminate security weaknesses.
3. Create an emergency plan that covers:
    a. Physical security
    b. Cyber security
    c. Asset security
4. Promote and update the plan.
5. Educate personnel about the plan.
6. Test the plan.

To identify security strengths and weaknesses, obtain a vulnerability assessment for your firm, preferably from a certified security consultant. Firms in the security/life safety industry are generally concerned with preventing personal, physical and information system loss. Security firms provide these security-consulting services, in addition to making and distributing security products.

The cost of a vulnerability assessment ranges from under $20,000 for a midsized company, to $1 million or more for a large international corporation [7]. You can expect a security consultant to create contingency plans for protecting employees, customers and assets; recommend locations for back-up offices and communications, firewalls, anti-hacking defense, and backup of data systems for cyber-security; and suggest procedures for employee and subcontractor background checks. Your security consultant will also warn you against suspect "security" products, such as parachutes for skyscraper evacuation, and personal radiation detectors.

To the extent possible, any weaknesses should be reduced or eliminated. A concise emergency plan should be developed that addresses the security strategies summarized in Exhibit 2. Then, make it available to everyone in the organization – on line, in print, in daily conversations – and update it every six months. Educate and train personnel – the management team, line employees, staff – about the plan so they can competently act if catastrophe strikes. Conduct crisis simulations at the company from time to time to test the plan.

Physical Security

Increasing the protection of physical premises includes actions such as reinforcing doors and windows, securing access to buildings and parking areas to protect employees, customers, and assets. Many firms have shatter resistant windows, fluorescent stripping on floor borders and stairwells, stairwell emergency lighting, better-trained security guards, regular bag checks, weekly alarm tests, remote back-up data centers, emergency

[7] Magnusson, P. (2003, April 14). Your jitters are their lifeblood. Business Week, 41.

water and power supplies, emergency evacuation plans, and even whistles for employees to blow in case of injury or entrapment [8].

Trucking companies are conducting more rigorous background checks for new hires, photo or unique employee ID systems, and cell phones for all drivers. Airlines prescreen frequent fliers using a system that contains passenger profiles [9]. Facilities and building managers, concerned about the threat of chemical and biological attacks in buildings, may install air filtration systems and enhanced control of air exchange. Multinational corporations (MNCs) have moved or may move facilities from high-risk locations, such as Indonesia, the Philippines and Malaysia [10]. Exhibit 4 summarizes actions that ensure physical security.

Exhibit 4
Physical Security

- Reinforce physical structures.
- Secure access to premises.
- Use safer materials.
- Perform employee background checks.
- Train employees for emergency.
- Prepare evacuation plans.
- Restrict travel to dangerous locations.
- Locate operations in safer places.

Cyber Security

Cyber security requires investing in upgraded servers and software, and creating back-up systems and off-site remote operations to protect against information system breakdown. One executive recruiting firm made it possible for its business to be

[8] Fannin.
[9] Varon.
[10] Lopez, L. & Saywell, T. (2002, October 16). Some foreign firms in Indonesia take steps to augment security. Wall Street Journal, A18.

conducted anywhere by moving its back-up information technology system offsite and by making software accessible to employees at home. Many banks have improved their emergency capability by creating new backup information systems, alternate physical sites and "virtual command centers" that can be ratcheted up to speed in minutes.

Exhibit 5
Cyber Security

- Create back-up systems.
- Establish off-site remote operations.
- Make software accessible from offsite.

Asset Security

Asset security includes innovations that protect product integrity. For example, technology can reduce identity theft, protect against pathogens in food shipments, and increase the security of hazardous materials shipments [11]. The security issues in transportation are so critical today -- terrorism, sabotage, contamination and smuggling – that companies do not need federal arm-twisting to realize that they must reduce risk. Many transportation firms have changed internal procedures on their own to protect access to equipment and cargo. They are controlling vehicle key and cargo access, installing tracking and locking systems, securing terminals, providing fenced and gated parking, limiting facility access, and using geographic positioning systems (GPS) to locate trucks. Some international transportation companies send manifests electronically so they arrive prior to the cargo landing and ease customs clearance [12].

SARS/Health Hazard Planning and Response

[11] Rothkopf.
[12] Mele, J. (2002). Homeland security: Trucking's contribution. Fleet Owner, S4-S10.

Companies such as Wal-Mart have used several alternatives to traditional buying to avoid sending buyers into SARS affected areas (Exhibit 6). Buying occurs via technology rather than face to face. Designers communicate detailed product specifications such as the cut of a shirt and the width of a shoe through email. Managers hold virtual meetings through videoconferencing. Wal-Mart asked suppliers, primarily from Asia, to fly into Dallas to exhibit, negotiate and sell products to Wal-Mart. The company does not plan to decrease its sourcing from China, but it is considering relocating two of its four annual Asian sourcing summits to the U.S. [13]

Exhibit 6
Purchasing Alternatives to Travel to SARS Affected Countries

- Videoconferencing.
- Digital photography transmitted via email.
- Detailed specifications and negotiating purchases via e-mail.
- Computer-assisted designs sent via Internet.
- Online trading and auctions.
- Express-mailing samples and communicating electronically.
- Suppliers going to buyer's location.
- Quarantine of travelers from affected areas prior to meeting with company personnel.
- Alternative sources of supply.

Although important face-to-face contact may be lost between buyers and suppliers, there are advantages to the alternative buying approaches. Videoconferencing is a faster and lower cost method of doing business. The average cost per diem for domestic travel is $663 compared to an hour-long Web conference cost of $60. In 1999,

[13] Kahn, G. & Zimmerman, A. (2003, May 18). In age of SARS, Wal-Mart adjusts global buying machine. Wall Street Journal, B1.

J.D. Edwards trained its sales teams in 17 offices using videoconferencing, and reduced the cost from $35,000 to $5,000.

To enhance videoconferencing, the best technological visual aids should be used. Companies should invest in videoconferencing technology such as enhanced lighting, ability to pan and zoom in on products, and better resolution video. Voice transmission through Web conferencing is not yet completely intelligible, but new software from companies such as WebEx may make this service as reliable and convenient as telephones. The Internet is another substitute for face-to-face meetings, but Internet communications can lead to miscommunication. After receiving the wrong item, one company overcame problems by emailing digital photos of the component they wanted to buy.

To protect staff, Wal-Mart asked suppliers from China, Taiwan, and Hong Kong not to meet with buyers until ten days after their departures from Asia. Passports were spot checked to assure compliance, and vendors who tried to cheat were turned away.

Asian suppliers had to modify their cultural preference for conducting business in person. Smaller retailers also had to adapt their buying practices. Some formed buying groups to increase their bargaining power. Many email digital photos and spreadsheets of product specifications, or put them on a CD and express mail them to suppliers.

A Kmart executive commented that while face-to-face contact in the showroom is critical, buyers who traditionally visit shows two or three times a year are discovering they can do business in one visit. Nike footwear is produced in plants in China, Indonesia, Thailand and Vietnam. By substituting e-mail, telephone, or video

conferencing, Nike has cut its business travel to Asia by 50%. Plant managers send samples via FedEx and communicate new designs with computer-aided design software. The company has a contingency plan to send production to Latin America should the SARS crisis worsen in Asia.

Final Comments

There is nothing static or stable about the threat of catastrophe. In the post-9/11 environment of increased physical threat of known, unknown and unknowable risk, CEOs must adopt a dynamic and strategic approach to risk management [14]. CEOs should network with their peers about how to manage catastrophe, although they may be reluctant for fear of revealing corporate vulnerabilities or security contingencies to competitors [15]. Finally, CEOs can take cues from the Security Taskforce of the Business Roundtable and their list of best practices for crisis management [16], summarized in Exhibit 7.

Exhibit 7
Best Practices for Crisis Management

- Make a full-time commitment to crisis management planning.
- Designate staffing and infrastructure back-ups.
- Address terrorism as a global concern.
- Keep vendors and customers in the loop.
- Don't just look at cyber threats but at the corporation as a whole.
- Develop guidelines for managing the crisis locally if communications with global headquarters breaks down.
- Assemble a crisis management team and lay out guidelines on who is chair of the group, how it is called into session, how decisions are made, who keeps a record of decisions and who tracks compliance.
- Test the crisis management plan.
- Keep risk assessments and contingency plans current.
- Review major sites globally to assess exposure for people, plants and records.

[14] Underwood, J. (2002, November-December). Corporate counter-terrorism, intelligence and strategy. Competitive Intelligence Magazine, 15-18.
[15] Papmehl, A. (2002, March). Business in an uncertain world. CMA Management, 12-15.
[16] Fannin.

- Protect operations visible to the outside by rotating schedules and routines so patterns can't be discerned.
- Make sure local managers of overseas locations are informed of developments unfolding elsewhere.
- Conduct mock drills regularly.