



WARNING: CRISIS AHEAD

Aug 1, 2008 12:00 PM, By Ashley Roe

Disasters are all around us. Last March, an outbreak of tornadoes barreled through downtown Atlanta, catching residents, tourists and businesses off guard and in harm's way. In June, hundreds of people were forced to evacuate when major flooding damaged homes and businesses in southeastern Iowa. This summer, wildfires have threatened areas of northern California.

In addition to such events caused by nature, there are also risks from disasters such as terrorist attacks, workplace violence incidents, explosions or accidents.

The potential for disaster clearly should be top-of-mind for business leaders, including security directors. A business continuity/disaster recovery (BC/DR) plan should therefore be a priority.

However, since recent events have not been as extreme as Hurricane Katrina or the Sept. 11 attacks, some company leaders have allowed preparedness to be pushed to the bottom of their to-do lists. Not a good idea.

Make planning a priority

Two recent surveys - one conducted by the Ad Council on behalf of the Department of Homeland Security's (DHS) Ready Business group and another administered by Boston-based technology research firm, Aberdeen Group - suggest that BC/DR planning progress among small-, medium- and large-sized private businesses is lagging.

The Ad Council's December 2007 survey of private businesses with two to 999 employees found that 91 percent of respondents believe it is "very" or "somewhat" important for businesses to take steps to prepare for a catastrophic disaster, such as an earthquake, hurricane or terrorist attack. However, only 38 percent said their business had an emergency plan in place in the event of a disaster.

The Aberdeen Group's survey, conducted between February and March 2008, examined the usage trends, experiences and intentions of more than 150 enterprises of various sizes that had already created some type of BC/DR plan. According to the study, 34 percent of the businesses surveyed were "in varying stages" of creating a business continuity plan and had yet to implement it.

So why aren't organizations getting prepared?

One factor, says Rebecca Marquis, deputy director of DHS's Ready Campaign (ready.gov), which strives to help individuals and businesses adequately prepare for and respond to emergencies, is complacency. "Aside from the recent flooding in the Midwest, we haven't had another 9/11 or Hurricane Katrina, and a lot of people have become complacent as a result. They are not thinking about preparedness as much as they should."

Adds John McCarthy, a principal of the Business Security Advisory Group (BSAG), a corporate security consulting firm established by five former chief security officers from major global corporations, and a Security Executive Council (SEC) member: "It all depends on whether or not people are taking notice of the risks around them. People ask themselves 'do I really believe a terrorist attack could affect me?' After 9/11, people did believe there was a real risk." But, McCarthy explains, as the years have passed since the Sept. 11th attacks, concern over the risk of terrorism among businesses has subsided.

Many business leaders take a misguided approach to BC/DR planning, says Scott Watson, vice chair of the ASIS Crisis Management and Business Continuity Council, and principal consultant of S.A. Watson & Associates LLC. "A lot of organizations approach crisis management planning from a compliance mindset," he says. In other words, business leaders spend time creating a plan simply in order to satisfy a requirement. In addition, organizations should spend time testing and adjusting the plan to make sure it will function well if it is called into action. Planning from a compliance standpoint, Watson says, too often involves developing the BC/DR plan, putting it in a binder and setting it on a shelf where it might go untouched or even forgotten about.

The need to demonstrate a clear return-on-investment (ROI) to senior business leadership may also be slowing businesses' approach. "Spending money on business continuity does not have an ROI associated with it, and if you don't see an ROI, many companies don't want to spend the money," says Frank Mahdavi, chief strategy officer of MIR3 Inc., a San Diego-based provider of Intelligent Notification systems for use in disaster recovery and business continuity processes as well as for general business and information technology practices. MIR3 was one of three underwriting companies that commissioned the Aberdeen Group's business continuity survey.

A fourth reason is cost. "These plans are not cheap to put together. They take a lot of time and energy, and if you are going to practice them on a somewhat regular basis, they require a lot of resources, too," McCarthy says.

Planning: Rules of thumb

Where does an organization begin to create and/or to build upon an existing BC/DR plan? There are some general rules of thumb to take into consideration.

The ASIS Crisis Management and Business Continuity Council, an educational group that promotes best practices in crisis management and business continuity, organizes an annual three-day workshop dedicated to basic crisis management training, including instruction of the "Six Steps of Crisis Management."

During the workshop, Watson explains, groups of participants take part in role-playing exercises, with each group representing a fictional company in a fictional town, and each participant is assigned a fictional role within the company. Participants are taught how to create a crisis management plan using the six steps as a guide.

"Our students get a good foundation for understanding the process of creating a plan, including the experience of working with various groups representing an organization," Watson

says. "Participants can then bring their notes and knowledge back to their respective organizations for use in developing their own plans.

Know the six steps of crisis management.

1. **Begin the strategic planning process**

Involves getting and giving executive support for the program, determining the scope of the program, establishing a crisis management team and determining a budget.

2. **Perform a risk and business analysis**

Involves determining the types of risk the organization must have protection from and the best means to do that.

3. **Develop the basic elements of the crisis management plan**

Involves writing an executive summary and authority statement and naming specific crisis management, incident response and business recovery contacts.

4. **Determine the tactical elements of the plan**

Involves determining the specific courses of action individuals will take on the front lines during the actual disaster.

5. **Exercise the plan**

Involves practicing the plan on an annual basis. The ASIS council uses the tagline: "An untested plan = No plan." Watson recommends that every organization practice its plan at least once per year, depending on a number of factors such as impending risk, incident history, size of the organization and experience level.

6. **Revise the plan**

Involves incorporating lessons learned from an exercise into a revision of the plan. "The crisis management plan is never complete," Watson says. "It's a cycle. You develop the plan, practice it, iron out the problems, revise it, and then start over from the beginning."

In addition to knowing the six steps, BSAG's McCarthy, who is a former global director of corporate security for Texaco Inc., adds a few more guidelines.

Start with an evacuation plan

"The first part of a good disaster plan is a good evacuation plan," McCarthy says. "There have to be adequate avenues of escape in place, and you must be sure to provide for employees who are disabled or have other special needs." Along with this, organizations must plan for what happens to their employees after evacuation, such as designating a safe holding area and meeting place, providing medical services if needed and supplying food and water.

Appoint a crisis manager

"The crisis manager has to be a good team leader and coordinator. He or she must have knowledge of the business unit, be able to deal with a crisis and know the employees,"

McCarthy says. Adds Watson, "The crisis manager also needs to have good analytic skills. He or she has to be able to make decisions under pressure, to allocate the appropriate resources and to know when response needs to be increased at any given time. They also need an ability to reach out to other organizations for assistance, if necessary."

In some cases, security directors are appointed crisis managers because of their wide overview and knowledge of the entire organization, their ability to incorporate a crisis plan into each business unit and their skills for development and implementation. Other organizations, McCarthy says, might appoint a manager from the corporate services department because its employees generally oversee and control all facilities within the company and have experience dealing with a number of departments. A manager from the company's human resources department is also a consideration because of his or her deep knowledge of employment processes, payroll procedures and conflict resolution. "This decision all depends on how the company is situated and what its philosophy is," McCarthy says.

Develop a business resumption plan

"This includes all of the tasks encompassed in putting a company back together again," McCarthy says. The crisis management team must decide where the organization will be temporarily relocated and which employees will be working at the new location. They must also determine what happened during the disaster and assess short- and long-term effects on business departments and components. Keeping the communication lines open with the company's suppliers and clients is also included in the plan.

Appoint a public relations contact

Depending on the type of disaster that occurs, media members may take notice and arrive to report the story. "Journalists can often be very aggressive. They have a job, and they have deadlines to meet. If this is a big story, they are going to want details," McCarthy says. "Companies should set up a space in order to brief the media, and often. Supply them with the facts. If you don't, they will begin interfering with your job during disaster recovery."

An effective public relations team can also work to make sure employees' family members have the latest critical information available. In addition, they can communicate and keep the company's customers and clients informed and up to speed on recovery efforts. "Showing your customers that you are responsible and attentive and can handle a disaster can result in their increased loyalty in the future," McCarthy adds.

Provide emergency training to all employees

Basic disaster training for all company employees can ensure that everyone knows what to do if disaster strikes. "Your people have to be trained. They have to know about emergency plans," McCarthy says. "If they already have the plan ingrained into [their heads] and they can do it in their sleep, they are going to act in an orderly manner [when the time comes]."

Watson recommends companies take a multipronged approach to educating employees. This might include posting emergency training literature on company Web sites or sending out company-wide e-mails with emergency information. Larger organizations may also follow in the footsteps of Atlanta-based Cox Enterprises Inc., which created CoxAlert.com, a comprehensive online emergency resource for its employees. (See "Case Study: Cox Enterprises Inc." sidebar.) "Another idea is to schedule brown bag lunches and give an emergency training seminar at lunchtime," he says. "Also, find a way to link this training to your employees' individual needs and responsibilities. If there is a personal interest there, employees are more apt to absorb and understand the importance of the training."

Partner with local government entities and neighboring organizations

"You want to make sure that things are interoperable," Watson says. "If you have a big enough disaster happen, the public authorities are going to be involved. You are going to need knowledge of the U.S. Incident Command System (ICS) and of the National Incident Management System (NIMS), and this is achieved by developing relationships with your local leaders."

Watson suggests one way to begin the familiarity process. "Invite leaders out to lunch. Or get involved in some way on a local level," he says. "There are lots of organizations that do not reach out to local authorities, and these relationships can really help in the long run."

Adds McCarthy: "Don't forget about your neighbor. It's okay to partner with neighboring companies and organizations in times of disaster." For example, groups of companies located in multi-tenant buildings might coordinate their emergency evacuation and response procedures to ensure a smooth execution when disaster strikes.

Additional resources for success

There is an abundance of disaster management and business continuity training guides, tip sheets, publications and training programs, including the following:

NFPA 1600 — Most recently revised in 2007 (the next revision is planned for 2009), the National Fire Protection Association's Standard on Disaster/Emergency Management and Business Continuity Programs is a comprehensive guide to developing BC/DR and emergency management programs for public, non-profit and private organizations. The document discusses the criteria for assessing current programs and developing, implementing and maintaining aspects for prevention, mitigation, preparation, response and recovery from emergencies. Visit nfpa.org.

Ready Business — An online resource created by DHS and the Ad Council in 2004 that provides information to help owners and managers of small- to medium-sized businesses prepare their employees, operations and assets in the event of an emergency. The Web site provides businesses with practical steps and easy-to-use templates to create an evacuation plan, implement fire safety procedures and protect business investments by securing facilities and equipment and by reviewing insurance coverage.

Marquis says the resource is catered specifically to small- and medium-sized businesses because according to the U.S. Small Business Administration, small businesses represent more than 99 percent of all employers, provide 75 percent of the net new jobs added to the economy and represent 97 percent of all U.S. exporters. "Our ideology is that if these businesses are prepared to survive and recover, the nation and the economy are more secure," she says. Visit ready.gov/business.

"On The Brink: Re-engineering the Nation's Disaster Response Processes" — In July, the Business Civic Leadership Center of the U.S. Chamber of Commerce published a new report that offers expert analysis, lessons learned and recommendations for disaster management processes among public and private entities. The collection of 27 articles includes essays penned by emergency-response professionals representing corporations, local chambers of commerce, federal and local government, academia and humanitarian-aid organizations. Visit uschamber.com/bclc.

National Emergency Response and Rescue Training Center (NERRTC) — NERRTC, a part of Texas A&M University's Texas Engineering Extension Service (TEEX), has provided public and private sector emergency response leaders with hands-on, scenario-driven, emergency response training and exercises to prepare for terrorist attacks since 1988.

Currently, the center offers approximately 20 classroom and online courses in areas such as emergency management, incident command training, emergency operations, leadership development and risk/threat assessment, says Harrison Lobdell, NERRTC national director.

Included in the curriculum, students learn the acronym "POETE," which stands for Planning, Organization, Equipment, Training and Exercise, and use the concept as a guideline for preparedness training and disaster response exercises. NERRTC also boasts a 120-acre fire training field, a 52-acre urban search-and-rescue training facility and a 31,000-square-foot fully functioning emergency operations center where scenario-based training is conducted Visit teexweb.tamu.edu/nerrtc.

Hazard Tactics Training — Presented by Prepared Response Inc., Seattle, in conjunction with the Community Safety Institute and the Washington Association of Sheriffs and Police Chiefs, the Critical Incident Management Consortium (CIMC) training curriculum - also known as Hazard Tactics Training - offers customized training in multiple national safety initiatives and multi-hazard emergency operations. The curriculum includes courses on threat assessment and prevention, communication during a crisis, pandemic and bio-emergency management training, business continuity planning, creating a crisis response plan, developing an all-hazard planning team and more. The program also offers courses in NIMS and ICS. Visit preparedresponse.com/training.

Emphasize Communication — By far, Marquis says, the most important component of an effective BC/DR plan is communication.

CASE STUDY: COX ENTERPRISES INC.

"Businesses should take a proactive approach to disaster management and business continuity planning rather than a reactive approach," says Bob Brand, vice president of corporate security for Atlanta-based Cox Enterprises Inc. This includes developing a certain amount of foresight into the consequences an organization can anticipate with each type of disaster that poses a risk.

With roughly 83,000 employees dispersed across six major subsidiaries throughout the United States and abroad, Cox Enterprises spearheaded its proactive planning approach by creating a comprehensive online resource for employees - CoxAlert.com - that serves as a guidebook to emergency preparedness and management. Cox employees can visit the site and receive regular updates on natural disaster threats, guidelines for preparedness for a number of emergency situations and to review prepared plans of action for use before, during and after a variety of natural and man-made disasters.

"The CoxAlert tool was created shortly after Hurricane Katrina because we realized we needed another way to reach out to our employees during a crisis," Brand says. "With critical information already at his or her fingertips, the employee is better prepared. They can then share the information with their families and reach a wider audience, and their families will be more prepared. Eventually, the entire community will be more prepared."

Cox Enterprises learned another lesson from Hurricane Katrina. After the storm moved ashore on Aug. 29, 2005, the company scrambled to make contact with 400 missing employees in the affected Gulf areas. Cell phone service was knocked out, further complicating efforts to reach employees located in the storm's path. "Often times you cannot depend on cell phones and other mobile devices for communication during a disaster," Brand, who is a member of the Security Executive Council, says. As a result, Cox Enterprises created a toll-free (800) number to allow employees to check in and report their status from anywhere in the world after an emergency or crisis.

Cox's online emergency resource is accompanied by daily risk analysis e-mail reports sent to senior leadership to keep them better informed. "We report on labor issues that might affect

us, travel advisories, medical alerts, national hazards, weather alerts and more," he says. Additionally, Cox requires each of its core businesses to appoint a business continuity director, develop a business continuity plan and practice it at least once per year. Brand's team evaluates the plans every year using a red/yellow/green grading scale.

The company's internal policies are further supplemented by BC/DR technology, including emergency notification services from Send Word Now Communications, New York, asset monitoring and risk assessment solutions from iJet Intelligent Risk Systems, Annapolis, Md., and continuity planning software from COOP Systems, Herndon, Va. "All of these solutions are what we refer to as our umbrella of crisis management," Brand says.

Crisis Management Technologies

A new class of crisis management software technologies are helping businesses unify their BC/DR plans, interoperate with emergency responders and communicate with employees to keep them informed.

"Virtual" Emergency Operations Center

More than a decade ago, Augusta, Ga.-based ESI introduced WebEOC, a Web-enabled crisis information management software. The WebEOC system is an incident-based information management system capable of managing ongoing events simultaneously and separately. Security directors and other users can track individual or multiple incidents through a common master view on the platform. In addition, the tool allows user to exchange critical information across multiple disciplines, jurisdictions and data formats.

"WebEOC is a tool that creates a common operating picture, allowing security directors and first responders to share information about incidents and make sound decisions quickly," says Nadia Butler, ESI CEO. "The unique ability of the WebEOC status boards to create real-time situational awareness enables security directors to direct resources when and where they are needed during natural and human-induced crises." Example status boards include those that track significant events using real-time chronology, mission/task assignments, infrastructure status and available resources. Visit esi911.com.

Critical Infrastructure Information System

Rapid Responder from Seattle-based Prepared Response Inc. provides first responders with instant access to critical facility information to help save lives and protect property. The Web-based system is used to create a digital catalog and inventory of critical infrastructure within public and private buildings, transportation systems, hospitals, utilities, schools, bridges and other structures. Using Rapid Responder, police, fire and other first responders can instantly access more than 300 data points, including tactical response plans, evacuation routes, exterior and interior photos, floor plans, utility shut-off locations and hazardous chemical inventories for nearly any facility.

Certified by the Department of Homeland Security's SAFETY Act, the system also facilitates the planning and mitigation phases of an emergency. Users can develop and update emergency response plans for multiple locations, distribute critical information to specific agencies via a secure Internet connection, view up-to-date emergency response plans and revise and update contingency plans. "All of this information is immersed within the system and is made available to first responders and corporate stakeholders," says Jim Finnell, CEO and president of Prepared Response, adding that having critical information, which can be accessed in a hurry, stored at your fingertips greatly increases the time for effective emergency response. Visit preparedresponse.com.

Intelligent Notification System

The inEnterprise communication system from San Diego-based MIR3 Inc. is built on a geo-dispersed, scalable telephony and application server platform that directs the global dissemination of time-urgent information to and from any communication device across any communication medium. The secure, role-based notification platform integrates seamlessly into an organization's enterprise communication infrastructure. It works in conjunction with standard corporate databases to allow organizations to consolidate emergency and routine communications across all divisions into a single intelligent notification platform.

When integrated with Microsoft Office Outlook, inEnterprise has the ability to deliver high-speed consolidated and acknowledged communications via landline, cell phone, e-mail, pagers, SMS, fax and satellite phone to individuals, groups, or company-wide to the desktop with the click of a button. According to the company, the ability to integrate across organizational divisions simplifies the deployment process and decreases the upkeep time spent on maintaining the integrity of the notification system.

"This system has replaced the traditional call trees of the past," explains Frank Mahdavi, MIR3 chief strategy officer. "With this automated solution, users can convey a number of tailored messages to different people. The security department can receive one message, while management gets another and so on. This is something that was not possible with the traditional call tree." Visit mir3.com.

Terms To Note

Disaster - 1.) A sudden unplanned catastrophic event causing unacceptable damage or loss. 2.) An event that compromises an organization's ability to provide critical functions, processes or services for some unacceptable period of time. 3.) An event where an organization's management invokes their recovery plans.

Emergency - An unexpected or impending situation that may cause injury, loss of life, destruction of property or cause the interference, loss or disruption of an organization's normal business operations to such an extent that it poses a threat.

Disaster Recovery - The ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions.

Emergency Response - The immediate reaction and response to an emergency situation commonly focusing on ensuring life safety and reducing the severity of the incident.

Disaster Recovery Plan - A management-approved document that defines the resources, actions, tasks and data required to manage the technology recovery effort. Usually refers to the technology recovery effort. This is a component of the Business Continuity Management Program.

Business Continuity - The ability of an organization to provide service and support for its customers and to maintain its viability before, during and after a business continuity event.

Business Continuity Plan - The process of developing and documenting arrangements and procedures that enable an organization to respond to an event that lasts for an unacceptable period of time and return to performing its critical functions after an interruption.

SOURCE: DISASTER RECOVERY JOURNAL AND DISASTER RECOVERY INSITUTE INTERNATIONAL GLOSSARY

