

Disaster Management

Testing Murphy's Law

By Ken E. Reid, CPP

A contingency plan is only as good as the company's last drill.

Disaster can strike any time, anywhere. Workplace violence, fires, arson, tornadoes, hurricanes, flooding, terrorist acts, hazardous materials spills--all are possible, some nearly commonplace. By implementing a continuous program of testing and role-playing, safety and security professionals involved in contingency planning can dramatically improve their organizations' chances of cutting loss when a disaster strikes home turf.

Many organizations and businesses understand that contingency planning is vital, and they already have established such plans. Policies and procedures have been created; estimates on duration and cost of potential incidents have been worked out; and contact lists, protocol, and procedures for obtaining outside resources have been put in place. The final draft of the plan has been approved, printed, and returned for distribution; copies have been circulated, and everyone feels confident that the organization will be prepared to cope with any emergency. Unfortunately, this is too often the end of the process. The contingency plan ends up filed behind other documents and is eventually forgotten--forgotten, that is, until the disaster actually occurs. It is then, when a functioning plan is most needed, that Murphy's Law will prevail: Everything that can go wrong, will go wrong.

The creation of a contingency plan is only the first step of an ongoing process of disaster planning, training, exercising, evaluating, and revising. As a part of this process, the security manager should also ensure that disaster preparedness has the continued support of senior management.

Practice may not make perfect, but it can at least make everyone more prepared to deal with the inevitable surprises. A company should plan for every contingency, but it helps to evaluate the most likely local threats to the facility and to practice those disaster plans specifically.

Many sources of assistance exist. Among the sources of information the security manager can turn to in developing the company's local disaster profile are the weather bureau and the local office of the Environmental Protection Agency, which can provide information regarding types, quantities, and locations of hazardous materials. In many states, advice and assistance can be obtained from local agencies as well, such as the Office of Environmental Resources located in each county in California. The information such organizations maintain includes types, quantities, and locations of hazardous materials stored in the area.

Acting out.

Testing of the emergency plan reveals inevitable unforeseen problems. For instance, role-playing exercises may identify conflicts, overlaps, and gaps in the chain of command. In addition, periodic test runs ensure that contact information and procedures stay current and that the plan remains fresh in the mind of every company employee.

Generally, the larger an organization, the more frequent and detailed the practice runs should be. At a minimum, the security manager should review the plan and training practices annually and conduct at least a limited practice run. Key decision makers who would be assigned to incident command should, as a committee, review the plan as well.

Prior to an exercise, the security manager or committee of key decision makers should send the affected departments a written request for the personnel, assets, and funding needed to meet exercise objectives. The security manager should also meet with managers of departments with key roles in disaster response and mitigation at least annually, prior to preparation of the budget for the next fiscal year to identify deficiencies or needs.

Based on experiences from prior exercises and the objectives of upcoming exercise plans, they should work together to identify items that should be included in that department's next budget request. These should be items that will not only satisfy the needs of the exercise but that may also be used in a real emergency--for example, computer software or hardware, sound-powered telephones, hand-held radios, status board materials, an uninterruptible power supply, or a generator.

Tabletop. Most organizations can test aspects of their disaster contingency plan through a "tabletop" exercise designed to introduce participants to basic plan operations and procedures. The exercise is usually played out at an accelerated pace, with all participants located in the same room and no actual movement of operational resources in the field.

Key decision makers are placed in their respective roles through a variety of role-playing situations. Whenever practical, the facility and equipment designated for command, communications, control, and documentation should be used as the setting. During the role-playing, a wide variety of situations should be explored to determine potential problems during multiple types of disaster incidents.

For example, in real-life incidents where major flooding occurred, many otherwise well-prepared organizations found themselves without any method of moving their key personnel and equipment over water. They also discovered that emergency operations and backup data processing centers were inaccessible because of the flood and no additional backup sites had been planned. These businesses not only lost all ability to conduct mitigating activities, but also lost all of their automated files.

Larger organizations should expand their testing to include a command center exercise designed to test command, control, communications, security, intelligence, documentation, and other elements of a disaster contingency plan, once again without the actual movement of operational resources in the field.

The tabletop exercise, as set out above, is played at an accelerated pace with only the key decision makers typically gathered around a graphic display or model on a table. In the command center exercise, however, the actual command center is used, as well as all the equipment and personnel that would be on hand during a real emergency. (In the case of businesses with assets spread out over a wide area, multiple command centers might be involved in this exercise.)

The command center exercise allows key personnel to practice their delegated duties and responsibilities while interacting with all other incident command center staff and equipment. Internal and external procedures and communications should be tested. Scenarios should include situations in which some key players are unavailable, since that is likely to occur during a significant disaster.

Large organizations often have command centers with several special purpose rooms, or even satellite facilities. Some have backup emergency operation centers with redundant capabilities; all of these should be tested.

Laptop. Virtually all aspects of a tabletop exercise can now be tested using computer systems. With the addition of other forms of communication and personnel, the command center exercise can also be entirely played out on computer systems. And even many aspects of a field training exercise (described in the next section) can be created and played out using computers.

Electronic testing of plans is accomplished using internal computer systems or linking distant computer systems through networking services--typically LANs and WANs. However, it is possible to extend the concept of "live chat" through America Online, CompuServe, or most local servers, via the World Wide Web, to include digitally simultaneous transmission of sound, graphics, video, and data.

In effect, it is possible through a local call at each user's end to have multiuser, real-time conferencing that goes far beyond simple chats. Anything created within the program running on the computer can be sent to the other addresses. Each site can take turns editing, adding information, or manipulating graphic symbols on map overlays. Decision makers at locations far removed from the incident can view the same scenario, then discuss responses to problems presented. Digitally interpreted text, graphics, or sound can also be sent through special modems that operate much like cellular telephones, and from there, via satellite, to other similar modems.

Currently, 28.8 DSVD modems and software such as Tiger 28.8 Multimedia, Newtalk 2000, or Teleport Platinum for the Macintosh allow digitally simultaneous voice, data, and graphics, which can be viewed and acted on from widely scattered locations. For users of Microsoft Windows 95, a free add-on called Microsoft Meeting can be downloaded from the Internet. The program is designed to facilitate multiuser computer conferencing, including voice and other audio, and offering real-time chat.

Many disaster situations can be simulated or recreated by off-the-shelf, plug-and-play software that can be tailored to the organization's specific needs. However, no ready-to-use software packages exist created specifically for disaster management purposes.

The Apple Macintosh 7.0 and Microsoft Windows 95 environments offer the widest potential for locating a plug-and-play package adaptable to the organization's needs. Any person familiar with these computer environments could create at least some practical disaster management tools. Most large organizations have systems managers and technicians who are trained to accomplish much more. It should be stressed that neither a programmer nor a graphic artist is necessary to accomplish these goals. The author, who had no special training in computers, was able to set up a functional play-testing system in the late 1980s using a Macintosh computer and Business FileVision, which has long-ago been replaced by more advanced and user-friendly software.

Using these off-the-shelf Macintosh and Windows packages, programmers can incorporate fully relational databases that allow the linking of data concerning personnel and resources to graphic symbols. Another option is a CAD program with 2D or 3D capability that also allows for databasing. One example of such software is MiniCAD Version 6 by Graphsoft (a Diehl product created for both Macintosh and Windows environments).

Such computer programs permit the incident manager or other decision makers to access a wide variety of information, then display graphic representations of resources on an automated status board much like a military battle table. Virtually all command center operations can be tracked, complete with date and time stamp for documentation. Data about resources, communications, logistics, and finances, for example, can be included in computer files.

The incident manager can click on a symbol and instantly see the information connected to it: the personnel manning the resource, when they were deployed, from where, with what mission, the cost factors, and any other data that is pertinent. The decision maker can click on the symbol and drag it to a new location, thus simulating redeployment.

The exercise can be tailored to meet the needs of both those making the overall decisions and those carrying out their instructions. For instance, responding personnel can manipulate figures representing themselves on the computer to illustrate how they would handle the situation. As they proceed up a stairway, for example, the computer screen can show not only where they are, but can depict what they would see from that position.

Training exercises that allow a facilitator to escalate or decelerate situations based on the measures taken by the player can be developed, similar to the Firearms Training Simulation (FATS) "Shoot-Don't Shoot" modules for law enforcement and security officers. Extending that concept, line personnel can be tested for ability to respond to the handling of fires, hazardous materials incidents, floods, and other problems.

For example, in a scenario depicting a chemical spill, known factors like reactivity of the chemical to other substances and various appropriate and incorrect mitigation measures can be mixed with such variables as wind direction to test response capabilities.

Most of this software can also log every activity as it is occurring, for documentation. The information can be useful in calculating costs or in the case of a legal suit.

Highly detailed maps, typically on CD-ROM, can be purchased for almost any location in the United States. An example is Precision Mapping 2.0. Even complete nautical charts--including tides and currents--can be purchased for both the Macintosh and Windows 95

environments. Maps of facilities and the area of concern around them can also be easily digitized by scanner or drawn with a variety of easy-to-use CAD-type programs, including some designed specifically for law enforcement and security.

An incident command center status board can be created on the computer, showing location and type of resources applied to the problem, staging areas, and routes to the incident. As obstacles are created by a facilitator, alternative routes and measures can be readily accessed for consideration. During a real emergency, alternative measures can be considered and tested using this method prior to actual deployment.

If talent exists in-house or the organization can afford a designer, an example of a scenario that could be created with CAD 3-D software is the response to a report of an armed ex-employee in the facility. Scale graphics, 3-D models, and even digitized photos or video of the interior of each compartment or space within the facility can all be included. Those tasked with crisis response can view the situation, make decisions, and deploy resources all without leaving the exercise room.

Another benefit of computer technology is that it can be used as a means of communication, even when the phones go down. Generators are often maintained as emergency backup by larger organizations. However, even the smallest businesses can afford uninterruptible power supplies (UPS). These are connected between the normal power supply and the computer. The UPS serves as a surge protector and also provides battery power when electrical current drops or stops. Laptops can also be used during emergencies to communicate if they are maintained with fully charged batteries and are equipped with wireless modems using a UPS.

Field testing. The largest and most complex organizations periodically broaden the testing process further to include a field training exercise. It tests and evaluates all elements of the contingency plan--policies, procedures, tactics, command structure, operations, logistics, security, intelligence, communications, documentation, and interoperability--through actual deployment of resources.

In these exercises, attempts are made by field operatives to actually carry out the decisions made by those in command. Field testing is costly and disrupts normal operations, but the benefits of the training and experience--including the inevitable discovery of plan deficiencies--is typically worth the temporary inconvenience and loss of productivity.

One problem often encountered during field testing is a breakdown in communications. Phones are often rendered useless during a disaster--if not from damage, then from system overload. Many organizations forget to arrange a backup, or they pick a type of system that is also easily damaged. For example, backup radio frequency (RF) communication can be crippled if the repeater has been knocked out. One large firm in the path of a recent tornado realized too late that equipment set aside for emergency operations was no longer compatible because the RF channel had been changed on equipment currently being used for normal operations.

One means of overcoming the loss of communication is to use computer distributed communications, or "trunking." From five to twenty radio channels might be used in the 800 MHz range, plus one channel for the computer. That way, emergency communications can be routed through a variety of repeaters by the computer. The chances of all repeaters being knocked out, even with widespread destruction, is substantially lessened. And as elementary

as it sounds, other organizations have realized during role-playing that radios stored for emergencies will not function properly without regular maintenance.

Another frequently identified problem is the procedural gap between identification of need and acquisition of necessary resources--a problem more apt to occur when the company is going to external public and private entities for services or equipment. Unless the security department or those persons selected to maintain the network of liaisons continuously reinforces formal and informal agreements, it may be difficult for the company to get help in a timely manner.

As many organizations have discovered during actual emergencies, some public agencies with emergency resources have no jurisdictional obligation to provide assistance during a crisis. A company should have a written agreement with all third parties that sets forth the resources to be provided, stating the purpose, duration, and the authorizing personnel. The agreement should include a release of liability on the part of any public agency. Legal council may suggest other issues that need to be addressed.

These agreements are called memoranda of understanding (MOU). An MOU is an agreement between a public agency and private company spelling out all the details of providing assistance in an emergency. (Security professionals may also be aware of Mutual Aid Compacts. However, these agreements are usually between public agencies to allow interterritorial operation--for example, when police districts agree to conduct law enforcement activities across each other's borders.)

Consider the recent widespread flooding along the Mississippi. Many cities and counties outside the flooded areas had departments, such as public works and fire departments, with equipment and personnel capable of providing flood control measures, including dike building and pumping. Unfortunately, many businesses and other organizations in the flood plain had not taken the time to negotiate MOUs and so assistance was not provided.

Another often forgotten procedure is negotiating purchase order agreements in advance--with businesses that rent heavy equipment, for example. In an emergency situation, time is critical to mitigating loss. To a facility on the bank of a rising river, the time spent negotiating purchase order approval with a supplier of sandbags could make the difference between suffering minimal loss and substantial damage to the company's property. What's more, the company that has not made advance arrangements for equipment, contract officers, or other forms of mutual aid may find that it is given the lowest priority during a time of crisis or that the companies providing these services and resources have no uncommitted time or materials to offer.

Disaster contingency planning is, fortunately, becoming widely recognized as essential to the well-being of any organization. However, a commitment to routine testing of these plans is more rare. Security managers should ensure that plans are practiced to protect their companies from the costly consequences of Murphy's Law.

Ken E. Reid, CPP, is president of Systems Concepts for Corporate Security, Modesto, California. He is also a lieutenant commander and special agent with the Coast Guard

Reserve, having served as a disaster contingency planner and exerciser. He is a member of ASIS.

A Room With a View

Security forces in stadiums and arenas practice crowd control as part of their everyday duties, but those skills are also of value in environments where mass gatherings are rare. A business, for example, may find itself the target of a curbside demonstration, and its security staff must know how to balance maintaining order with preserving its public image.

At a high profile event, such as a strike or demonstration, security will often be put on display by the media. Should the security team make one wrong move for a television camera or someone's camcorder, the fallout could be extreme in terms of damaged reputation and intense media criticism.

One key to effective crowd control is using an experienced officer to view the crowd from an elevated vantage point. Unlike the officers in the hurly-burly of a crowd, observers remain largely unthreatened, detached, and objective. In constant communication with a security supervisor in the crowd, this officer can help the security force adapt its response to an ever-changing situation.

It is also prudent to use a specially trained officer, rather than the supervisor, as the observer. This allows the supervisor to focus on the individual elements in the crowd and on controlling and organizing personnel.

An observation officer should be stationed as soon as a crowd begins to assemble. With the observer's guidance, line officers can be directed to possible trouble spots. The observer can also help choreograph the positioning of equipment, such as power lines, so as to avoid injuries. Guided by the observer, security's quick and organized response may well give pause to crowd members bent on bedlam.

Placement.

The observation point should balance safety and surveillance capability. Some key points include elevating the observer to provide depth in viewing the crowd; concealing the observer somewhat from the crowd (both for personal safety and to prevent the crowd from using the security team's surveillance activity as a rallying point); and providing the observer with an unobstructed means of egress so he or she can quickly assist fellow officers or escape trouble.

Observers should always be in a position low enough to hear the crowd.

An example of a good location for an observation position might be a partially opened second-story window in the part of the company's building facing the crowd. Such a location enables the observer to watch the entire gathering.

Communication. Observers are responsible for recording everything they see and hear, providing both a permanent record for later examination and real-time intelligence conveyed via radio to the supervisor and command post. To this end, the observer should be equipped with a radio, camera, and other appropriate surveillance equipment.

Via radio, the observer should provide a running commentary of information about the crowd, first to the supervisor and then to the command post when it is established. Having the observer communicate with the command post frees the supervisor to focus on controlling the situation.

Observers should also have a telephone with an outside line so that they can call for outside help or assist the command post with communications.

The observer should report objectively about both threatening and friendly elements in the crowd. A typical report might include some of the following:

- Size and relative condition of the crowd members
- Activities engaged in by the crowd and any individual activity of concern
- Exact location of the crowd's formation and the directions of the comings and goings
- Evidence of organizations with which crowd members appear to be affiliated
- Any equipment, tools, weapons, or other objects in the crowd's possession
- Whether the crowd has shown signs of any apparent leaders
- Whether the crowd has any support systems that may suggest a prolonged stay, such as water coolers, blankets, and first-aid stations
- Size, type, and location of security response and their vulnerability to the crowd

This information will be used by the command post to coordinate its plan of action.

An observation officer offers a great benefit without much cost in time and money. Observation training can be conducted easily with simple exercises. For example, an officer may be asked to observe cars passing through a busy intersection to train him or her to assess traffic patterns, incidents, and the like.

Establishing an observation point close to a crowd disturbance helps the crowd control team better organize a response, counter crowd activity by coordinated movements, and keep the command post continually updated from a safe position.

Robert Metscher, CPO (certified protection officer), PPS (personal protection specialist), recently served in South Korea as cavalry scout in the U.S. Army, where he periodically dealt with crowd control during demonstrations outside his camp.

Digital Resources

The following are digital resources on the Internet's World Wide Web and can be accessed simply by going to Security Management Online, pulling up this article from the library (or the links directory), and clicking on any item.

- Federal Emergency Management Agency: <http://www.fema.gov>
- U.S. Department of Agriculture Disaster Information: <gopher://zeus.esusda.gov:70/11/disasters>
- University of Illinois at Urbana-Champaign Cooperative Extension Service Disaster Recovery Information: <http://www.ag.uiuc.edu/~disaster/prepare.html>

- Natural Hazards Research and Applications Information Center, University of Boulder, Colorado: <http://adder.colorado.edu/~hazctr/intro.html>
- Emergency Preparedness Information Exchange Center for Policy Research on Science and Technology, Simon Frazer University, Vancouver, British Columbia: <http://hoshi.cic.sfu.ca/~anderson>
- British Columbia Provincial Emergency Program: <http://hoshi.cic.sfu.ca/~pep>
- Emergency Response and Research Institute: <http://www.emergency.com>
- Applied Technology Council: <http://www.atcouncil.org>
- Cascades Volcano Observatory: <http://vulcan.wr.usgs.gov>
- U.S. Geological Survey Landslide Information Center: http://gldage.cr.usgs.gov/html_files/nlicsun.html
- National Lightning Safety Institute: <http://adgrafix.iserver.com/nlsi/home.htm>
- Southern California Earthquake Center: <http://www.usc.edu/dept/earth/quake>
- Disaster Recovery Journal: <http://www.drj.com/>
- Internet Disaster Information Network: <http://www.disaster.org>
- The Disaster Connection: <http://www.itn.is/~gro/disaster>
- Disaster Recovery Internet Vendor Directory: <http://www.drj.com/drj5a.html>