People and Plans: Training's Role in Homeland and Workplace Security

Here's how some organizations and training functions are preparing for the unexpected.

By Eva Kaplan-Leiserson

Is your business

secure?

Homeland security. In the United States, you can't turn around without seeing mentions of it in the newspapers, on television, in metro stations and airports, in the workplace.

Stricter controls by the new Department of Homeland Security and its partners are firming up U.S. borders, making it more difficult for potential terrorists to enter the country. Other DHS agencies are analyzing threats, protecting high-profile targets, and coordinating first responders. But there is still a lot to be done.

One major area that still needs improvement is security in private industry. Although experts point out that U.S. business interests were targeted in the attack on the World Trade Center and in the distribution of anthrax through the U.S. Postal Service, a year after September 11 only half of organizations surveyed by SHRM (Society for Human Resource Management) had put tighter security measures in place. A 2003 survey by IT security firm mi2g found that about a third of companies interviewed still didn't have complete preparedness and business continuity plans.

Morgan Wright, manager of BearingPoint's homeland security and intelligence community sector, points to the lack of government regulations as the reason industry has been slow to jump on the security bandwagon. Companies are waiting for mandates, he says, so they don't take wrong steps and waste resources. But the government gives the responsibility back to the private sector, saying in the *National Strategy for Homeland Security* www.whitehouse.gov/homeland/book/index.html that the United States' tradition of limited government requires that businesses take the lead.

Overwhelmed with information and short on cash, your company may be hesitant to the point of inaction. But much can be done with readily available resources. An organization's people and plans—not exhaustive government directives or expensive technologies—are key. Regular people in regular companies will ensure that U.S. workplaces are prepared for the unexpected. And directly and indirectly, HR and training functions will lead the way. Are you ready?

The benchmarks

Certain types of organizations have a head start on heightened security and can offer best practices and lessons. Adam Bianchi of Cutting Edge Information, a business intelligence and research firm, says that companies in "high-capital industries" have been focusing resources on security for years. Large automotive, pharmaceutical, and energy companies, Bianchi says, have billions of dollars worth of reasons to address security: Any small glitch could cost them dearly. Also, many international organizations—oil companies, for example—have locations in hot spots around the world where terrorism is a constant threat, so they have years of experience dealing with the realities that many U.S.-based companies have just woken up to.

Some of the large corporations that CEI profiles in its in-depth report, "Corporate Security: Protecting Productivity" www.cuttingedgeinfo.com/reports/FL53_Security.htm, fall into the category of companies the U.S. government calls "critical infrastructure." Eighty-five percent of those companies, deemed crucial to the operation of the United States, are owned privately. Their importance to the U.S. people has earned them special attention and direction from the Department of Homeland Security. The 96-page "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets" www.whitehouse.gov/pcipb/phsyical_strategy.pdf defines roles and responsibilities both for industry and the U.S. government and offers security strategies and actions. An Office of Private Sector Liai-

Security is mostly a superstition. It doesn't exist in nature, nor do Avoiding danger is no safer in the long run than outright exposure.

Readiness

Do you know what to do in an emergency situation at work? Whether a crisis is an act of terrorism, workplace violence, or a natural disaster, it's important to be prepared. Take this quiz to assess your readiness.

True or False?

1) To control bleeding in yourself or someone else, keep the injured area level.
2) If threatened by someone with a gun, follow the person's directions.
3) In a fire, use the back of your hand to feel if a door is hot.
4) If you're trapped in debris, shout repeatedly so rescuers can find you.
5) One evacuation plan should be used for different types of emergency situations.

Short Answers

6) Name three supplies a workplace should have on hand in the event of an emergency.
7) Define "shelter-in-place." When should that strategy be used?
8) How much bottled water should you allow for each person to drink per day?

son www.dhs.gov/dhspublic/display?theme=37 created within the new Department of Homeland Security also provides guidance.

What can critical-infrastructure or multibillion-dollar international companies teach small and medium-sized everyday organizations? Primarily, that security can't be an afterthought. Top companies, CEI says, develop their security just as they develop research, marketing, or other key business initiatives, weaving it into their cultures. That means focusing on people solutions over technological ones and integrating security into everything a company does.

First steps

People and their knowledge, CEI says, are the most powerful tools in a company's security arsenal. But knowledge must be shared and put into action. Training can't be developed until a company knows its vulnerabilities and risks. A crisis-management plan must be practiced and rehearsed. For a company to make security a priority, HR and training managers must partner with company heads and security chiefs so that everyone pulls together with a common vision. Each component of a successful security strategy must be viewed as a company responsibility.

The following tasks, then, aren't just for training, security, or company execs. They are to-do lists—what experts agree on—for a coalition. Consider these steps to be a broad overview, and refer to the resources included for more detailed information.

Designate a security driver. Whether a company is large or small, one person must be the central authority for security efforts. In large companies, that often means hiring or promoting a chief security officer who sits at the executive table and oversees security efforts throughout the organization. CEI estimates that 30 percent of U.S. corporations have created a CSO position. Salaries for those execs can be as high as US$550,000. In some cases, CSOs report directly to the CEO. More often they report to HR, says a study www.ci-pinkerton.com/news/2003TSTSorder.html by security firm Pinkerton.

But many companies survive without a CSO. What's important isn't the title but that security has an upper-level champion to make company-wide changes, Bianchi says. In organizations that have no security department, the head of HR might take on the role. No matter who heads up security, he or she should exhibit certain traits. According to Tim Bowen, BearingPoint's security chief, and Michael Hershman, CEO of security firm Decision Strategies, the security driver should be

- open-minded—has the ability to assimilate information from a variety of sources and avoid stovepiping
- cooperative—encourages sharing and teamwork, working for a positive resolution to problems rather than creating hard and fast rules
- connected—has contacts in government and law enforcement who can supply information
- working from a global perspective—recognizes the importance of this even at a U.S.-based company
- skilled in verbal and written communications—able to sell programs to senior corporate management and the board of directors.

The main responsibility of the security driver, CEI says, is to safeguard the company from external and internal threats and protect employees, physical assets, computer networks, and intellectual property. Many heads of security also set travel policy, work with HR on applicant background investigations, lead internal investigations on fraud or harass-

the children of men as a whole experience it. Life is either a daring adventure, or nothing.—Helen Keller

Quiz

Answers:

1) False. Elevate the injured area above the heart if no bones are broken.
2) True. Maintain eye contact and keep talking while following directions. Never try to grab the gun.
3) True. Feel the upper, middle, and lower parts of a closed door. If hot, find another way out.
4) False. Shouting can cause you to inhale dangerous amounts of dust. Yell as a last resort; instead tap on a pipe or wall.
5) False. Evacuation plans should be developed for various incident scenarios.
6) Acceptable answers include first-aid supplies, flashlights, a battery-powered radio, batteries, bottled water, nonperishable food.
7) "Shelter-in-place" means staying inside at a present location to avoid contamination in the event of a chemical or biological attack.
8) Plan for two quarts to one gallon per person per day.

Sources/ *Jane's Workplace Security Handbook,* redcross.org, ready.gov

ment, and oversee the security awareness and training program.

Crucial to the success of a CSO or other director of security is buy-in and commitment from the CEO, experts say, demonstrated by budget, personnel, and a consistent message to the entire organization about the importance of security. It's key for the head of security to have the cooperation of all workers, Bowen says, to do his or her job effectively. In return, security chiefs have the responsibility to create policies and procedures that are in line with the vision of the company.

Assess vulnerabilities, threats, and risks. Usually the first step for the security driver is to determine the organization's vulnerabilities. A list of those quickly becomes an action list determining direction, CEI says. Possible vulnerabilities include lack of standard policies or training, outdated facilities security, open networks, and old passwords. Conducting a vulnerability assessment provides a baseline to work from, says Lenny Hall, adjunct instructor at the University of Findlay Center for Terrorism Preparedness ◁)) **http://seem.findlay.edu/terrorism.** Then, assess threats and identify risks.

The threat assessment identifies potential adversaries and their capabilities and intentions. Hall points out that there's a significant difference between making a threat and posing a threat: "Many people make threats," he says, "but few pose a threat." Businesses can't respond to every threat that's made with all of their resources; that would be costly and ineffective.

A risk assessment, as defined by South Carolina's report on best practices in workplace security ◁)) **www.llr.state.sc.us/workplace/workplacesecurity.htm,** measures the probability that a threat will result in an incident and evaluates the severity of the consequences from that incident. If an organization hasn't done a separate threat assessment, the risk analysis will often assess threats as its first task. Hershman includes an assets assessment (listing and prioritizing assets) as part of the risk analysis.

For companies already involved with the ISO certification process, ISO registrar BVQI has developed a security management system standard that applies management tools and techniques to security, following the same plan-do-check-act format as other ISO standards. Like processes developed by company security departments or security consultants, it includes vulnerability and risk assessments and then goes on to apply such management tools as internal auditing, training, preventative action, controlling documents, keeping records, and so forth ◁)) **email dchurch@bvqina.com** for a copy of the standard.

Create a crisis-management plan. Although not every company will have the same degree of risk, every company should have a crisis-management plan—not only for potential terrorist attacks but also for natural disasters, fires, and workplace violence. The goal of such a plan is to protect employees and the business while an incident is occurring and minimize the damage to both. *Jane's Workplace Security Handbook* suggests a close tie between the threat assessment and crisis plan, saying that security policies and procedures should be "based on the priorities identified by the threat assessment team."

One major portion of a crisis-management plan, *Jane's* says, is designating the team that will set security policies and procedures and the team or teams that will coordinate responses in various types of emergency situations. (Those two groups may be the same.) Depending on the size and distribution of your organization, the crisis-management team can include representatives from risk management, HR, IT, facility management, media relations, senior management, and local fire and police department representatives.

Other important elements of a crisis management plan, Hershman and Hall say, include

- determining types of emergencies that could occur
- designating evacuation routes and general procedures for each type of emergency
- identifying what people or organizations your company would depend on in an emergency and assessing realistically what help they could provide
- determining how to communicate to workers, their families, and the press during and after an incident
- identifying where money will come from for cleanup, medical bills, and worker family support
- determining what type of additional training workers need to implement the crisis plans.

OSHA (U.S. Occupational Safety and Health Administration) offers resources to help companies plan for crises. The publication "How to Plan for Workplace Emergencies and Evacuations" is available as a free download ◁)) **www.osha.gov/publications/osha3088.pdf.** OSHA recently appointed John Ferris as the new special assistant for emergency preparedness; he'll coordinate the various OSHA directorates to work together on security projects.

Create a business continuity plan. A BCP is a specialized component of a crisis-management plan that aims to keep a business running after a disaster. CEI defines business continuity as the "systems,

Only in growth, reform, and change, paradoxically enough, is true

facilities, and other infrastructure that allow the company to fulfill its obligations to customers, employees, and vendors." Most continuity solutions involve creating redundancies, Hershman says, in your communication systems, network systems, office space, and manufacturing facilities. It's also important to examine your supply chain security. What would your company do if one of your suppliers was attacked and wasn't able to deliver?

The BCP process isn't new to areas of the United States that have severe natural disasters. People in areas with a high threat of tornados, hurricanes, or floods have been examining business continuity long before September 11. However, the terrorist attacks did introduce a new wrinkle. Hank Christen, director of emergency response operations for technology consulting firm Unconventional Concepts, says that business continuity post-9/11 isn't just about having backup systems and buildings: The sad reality now, he says, is that "companies have to consider what they would do if half of their employees were killed."

security to be found.—Anne Morrow Lindbergh

Training-driven solutions

It can't be overstated how important workers are to a company's security preparedness. Many security experts list people as the number 1 factor in the success of a workplace security plan. In fact, research by KPMG (now BearingPoint) found that 70 percent of security breaches at companies are caused, directly or indirectly, by employee actions. That makes training the linchpin: If companies can change employee behavior, CEI says, they can tighten security quickly and cheaply. Here are ways the training function can take the lead.

Raise employee awareness. The primary goal in raising workers' awareness is to build the recognition that security is the responsibility of each and every person. A security plan is only as strong as its weakest part, and one small problem in one department is enough to destroy an entire organization. In the same vein, it takes just one observant employee to save a company from a disaster. Judd Green, president of security firm Green Consulting Group, points to the plane that went down in the Pennsylvania field on 9/11 as proof of how people can make the difference in avoiding a catastrophe.

It seems obvious that security policies and procedures are of little use unless they're communicated to employees, but a 2002 SHRM study ◁)) www.shrm.org/hrresources/surveys_published/HR%20Implications%20of%20the%20Attack%20on%20America.pdf found that a third of respondents whose companies had disaster plans had communicated the plan to employees either to a small extent or not at all.

CEI says that security awareness programs can be created and implemented by the training department, the security staff, or an outside consultant and should clarify and document what activities are allowed and not allowed and what penalties might be.

Train workers. It's not infrequent, Decision Strategies's Michael Hershman says, that he walks the streets of Manhattan and sees hundreds or even thousands of people standing outside a building. When he first saw that happening, he thought it was a demonstration, but he soon realized the crowds were workers practicing evacuation procedures.

The best plans, policies, and procedures are moot if they're not practiced, and that takes training. It's important to train not just after a crisis, experts say, but in the calm periods when nothing is happening. That's when people can concentrate best and absorb the material. OSHA's report suggests that companies train on crisis plans annually and when they hire new workers, change or introduce new processes or technology, or alter the layout of their facilities. OSHA recommends these topics:

- individual roles and responsibilities
- threats, hazards, protective actions
- notification, warning, and communications procedures
- means for locating family members in an emergency
- emergency response procedures
- evacuation, shelter, and accountability procedures
- the location and use of emergency equipment
- emergency shutdown procedures.

You may also want to train employees in first aid, but each organization should customize training, experts say, based on the specific needs of the company and its workers.

How to train is as important as what to train. Security experts emphasize the importance of repetition and retraining. Not doing so is expensive and ineffective for most skills; when it happens with crisis knowledge and skills, it's highly dangerous. OSHA recommends practice drills at regular intervals, even including interdependent resources such as fire and police departments if possible. After each drill, the company should gather workers and managers to measure its effectiveness, says the South Carolina report, asking what worked well and what didn't to improve procedures and plans. Other experts suggest such traditional evaluation tools as learner satisfaction measurements ("smile sheets"), pre-

or post-tests, or follow-up interviews to evaluate the training.

Joseph Kinney, security consultant and a former Marine who developed a Website of security resources www.safespaces.com, says that training goals should be different depending on a worker's level. Training for lower-level employees, he says, should be clear and simple and reinforced in manuals, Websites, and employee communications. Training for front-line managers and supervisors should include how to respond to employee needs in an emergency. Senior managers should have guidance in "developing the skills and resources to help the company deal cohesively with security issues."

Kinney emphasizes the importance of common sense and intuition, calling them crucial skills in survival situations, especially those involving the threat of violence. Many security professionals, he says, denigrate those qualities, but he has seen many situations in which they were ignored and people were hurt because of it. Kinney's advice on trusting intuition saved the life of his nephew, who worked in the second tower of the World Trade Center. When emergency personnel told people it was safe to stay in the building, the nephew got out. He followed his gut, and the advice of his uncle to always do so, and is alive as a result.

Get buy-in, and change the culture gradually. Implementing new security policies and procedures can be a change management issue, so it's important to make sure workers are on board. CEI recommends not bombarding people with tons of information at once. Effective awareness programs are gradual and long-term, Bianchi says. Taking six to 24 months to work through changing the culture will be more effective than giving people a checklist of 25 things that must be done next week. Bianchi suggests integrating security into corporate, department, and team goals. Some managers have security goals included in their performance evaluations, he says. Their pay is tied partially to whether their staff is following security protocols.

What you're hoping for, Bianchi says, is an aha! moment when people say, "I understand why this is important." That happens by training managers to explain to their staff the security vision, the company's security goals, and the reasons behind them. Set milestones, CEI suggests, so people can measure their progress and celebrate when they achieve various targets.

Consider enlisting experts. Many companies bring in outside security consultants to contribute best practices and shorten the learning curve. Even large companies with CSOs, Hershman says, often bring in consultants to help them with the many demands on the security function. A consultant can also be someone with a big-picture view that CSOs or security managers can bounce ideas off of. However, an outside supplier may not be as quick to understand industry-specific concerns.

Kinney says simple is best, so if a

Additional Resources

- Department of Homeland Security
  www.dhs.gov/dhspublic/index.jsp
- DHS's preparedness Website
  www.ready.gov
- OSHA resources on workplace evacuation
  www.osha.gov/dep/evacmatrix/index.html
  www.osha.gov/SLTC/etools/evacuation/index.html
- Emergency management training
  http://training.fema.gov/EMIWeb
- Information on the Community Emergency Response Team (CERT) program
  www.fema.gov/nwz03/nwz03_123.shtm

It must be admitted that there is a degree of instability which is inconsistent with civilization. But, on the whole, the great ages have been unstable ones.

—Alfred North Whitehead

consultant draws up a complex plan, it may be hard to implement. He also suggests caution. Experts are cropping up all over the place, looking at homeland security as a cash cow. Look for more than a slick sales pitch, Kinney advises. A good consultant should be able to change the values of the organization and the way it functions overall. That's challenging, he says, but necessary. Also make sure that the expert is a member of a recognized organization such as the International Association of Professional Security Consultants www.iapsc.org.

The funding issue

Although many companies recognized the importance of heightened security after 9/11, budget issues in a tight U.S. economy have hindered plans. But budget is the last thing (literally) organizations should think of in security planning, says Hall. First, you should do a threat and risk assessment and identify training goals, he says. Then plan backwards and determine how much money is necessary to fulfill those goals. What you *don't* do is say, "OK, we have $5000 to spend. What can we get for that?" The safety of your employees and business isn't something you can buy at a discount store.

Still, budget constraints are a genuine concern, and security must be a focus for many years to come. To maximize financial resources, CEI suggests 1) customizing your plans and training to get the most bang for your buck and 2) including security in your corporate growth planning in order to minimize costs and maximize effectiveness over time. In addition, organizations should take a hint from the *National Strategy for Homeland Security*, which advocates dual-use programs that improve security and advance other goals.

Just as putting up a sign on your front lawn, "Protected by [security company name here]," can be a deterrent, companies can make a big leap forward in security just by communicating policies and procedures, CEI says. People with malicious intent will think twice about committing an act of violence, and making the plans known will lessen workers' anxiety and reinforce their self-confidence.

There are other strong reasons to make security funding a priority—carrots and sticks. A carrot: implementing and communicating a security policy can create a large competitive advantage. CEI says that security can be a differentiator in a tight market and attract potential customers, employees, and business partners. A stick: If a company fails to plan and prepare for emergency situations, it could be considered negligent after an incident and be held liable in the event of worker injuries or deaths. Another stick: Companies without crisis management and business continuity plans are not only accountable to workers, but also to shareholders, who will demand answers when an incident interrupts business and damages competitive advantage, says DK Matai, the executive chairman of mi2g.

Toward understanding

Dave McIntyre, senior fellow of the think-tank Anser Institute for Homeland Security www.homelandsecurity.org, says that a major barrier to the United States combating terrorism is not understanding the problem clearly. It's not one set of "bad guys" trying to hurt U.S. citizens, he says. All of the "technology developed to allow productivity, connectivity, profitability, travel, and free flow of information is catching up with [the United States]," coming into the hands of people who mean citizens harm. The United States [and other countries], McIntyre says, will be dealing with for a least a lifetime how to secure themselves from new threats without hindering basic freedoms. "That's a huge challenge," he says, which will require a true interdisciplinary effort from all parts of society. Says Judd Green, "There hasn't be another time in American history when training has been so important." TD

Eva Kaplan-Leiserson *is news and development editor of* T+D*; ekaplan@astd.org.*

The New "Cheek-ohs"

There's a new title in Washington, D.C: CHCO, pronounced *cheek-oh*. These chief human capital officers were established per a provision in the 2002 Homeland Security Act. Each U.S. federal executive department and major agency was required to select a high-ranking official as its CHCO; his or her mission is to ensure that the agency recruits, hires, trains, develops, and deploys a diverse, highly skilled workforce. Each CHCO is responsible for creating and maintaining a performance culture in his or her agency, linking performance expectations to strategic goals and agency values.

The CHCOs from cabinet departments form a CHCO Council, also mandated by the Homeland Security Act. The 25-member council, which held its first meeting in June, is chaired by Office of Personnel Management director Kay Coles James. The council will provide human resources policy direction and insight across the U.S. government, suggesting reforms and legislative action. A CHCO Academy will offer traditional classroom courses as well as e-learning opportunities to the chief human capital officers to create a shared understanding of the position's responsibilities and share best practices.