



NEWS BRIEFS

No Lights, No Camera, Just Action

Most companies have emergency response and disaster management plans, however many of them are put away until either someone asks about it or it is actually needed. However, effective emergency plans should be updated and practiced in some form at least once every three months. Although training and testing do not have to take long, there are several different areas of emergency response that must be addressed, including internal and external communications, safety, coordination, and legal concerns. After determining what needs to be tested, a security manager can either develop their own test or hire an outside consultant to do so. While hiring an outside party is easier, developing an internal test is less costly. Managers should form a planning committee consisting of representatives from different departments, who will help determine the format and size of the exercise. At the beginning, companies may want to first plan small exercises that introduce employees to the training in a low-stress environment where the manager makes a presentation and possibly asks the audience questions. Later, companies can move onto full-scale tests that include more people and planning. The planning of full-scale exercises can be made easier by partnering with organizations, such as the state Homeland Security Department or the Red Cross, who can offer valuable advice.

Welcome, Visitors

Statistics from the National Center for Missing and Exploited Children say over 700 children are abducted daily, while the National Alert Registry lists over 500,000 registered sex offenders in the United States. Schools with a well thought out, strict, and reasonable visitor management plan in place give teachers and administrators the confidence to deal with such predators or other wayward individuals who may try to enter school facilities. Especially during early morning, lunch, and later afternoon hours, administrators should patrol the campus and scan access points to be sure that only students and volunteers enter the campus. Administrators must limit the number of daily visitors allowed on school grounds, and require all persons besides teachers and students to check in at the main office. Once a volunteer or guest has entered the office, personnel should check for a state-issued photo identification and keep such information on file, though it may reinforce security if digital photo technology is installed to capture images of all visitors and issue daily passes. Teachers, assistants, adult guests, and any other administrators must carry either a name badge or a guest pass at all times. This not only ensures that all non-students in the building have checked in and have a purpose for being there, but also helps children identify authority figures in the event of an emergency.

N. Korea Says Ready to Join U.S. in Fighting Terrorism

The North Korean government expressed gratitude towards the United States and vowed to assist in anti-terrorism efforts after a U.S. destroyer ship aided a group of Korean sailors off the coast of Somalia on Oct. 30, 2007. U.S. medics provided relief to wounded North Korean sailors who were injured as they attempted to fight off Somali pirates near the country's capital of Mogadishu, and the North Korean news agency KCNA said in a recent statement that the country was "grateful" to the United States. The news group described the episode as "a symbol of cooperation in the struggle against terrorism" between the United States and North Korea, which has been on a terrorism watchdog list since 1988, but will soon be removed from the list by Washington.

NEWS YOU CAN USE

FBI Director Targets the Internet's Top Dangers

FBI director Robert Mueller spoke on Nov. 6 about the dark side of the Internet and the army of experts working to battle the numerous online dangers. Mueller used the example of al Qaeda Web master Younis Tsouli to illustrate how infiltrated servers and scams can finance or aid terrorists. Tsouli broke into servers to steal bandwidth, mounted phishing schemes to access credit card accounts, and founded a Web site for terrorists. Mueller pointed out that the Internet is a target for attacks as well as a means for launching attacks. The "cyber blockade" of Estonia's federal and infrastructure-related Web sites in April 2007 was the example used by Mueller to illustrate this threat. Botnets and hackers continue to wreak havoc as well, from disabling power grids to stealing sensitive intelligence. However, cyber criminals are increasingly being found and prosecuted by specialists in Regional Computer Forensic Labs. But because a growing number of cyber threats are coming from abroad, more international collaboration on such investigations is essential, Mueller said. The FBI's Cyber Fusion Center is another valuable resource that lets cyber experts, federal agents, merchants such as Target and Bank of America, and others discuss security breaches and cyber threats. Finally, the FBI's InfraGard program works on the community level to let members share data about risks to their own businesses through a secure computer service. Almost 21,000 members--from small companies to Fortune 500 businesses--currently participate in this localized private sector partnership, according to Mueller.

ALERTS



CHESLEY BROWN COMPANIES

Security Condition SecCon 3



[Click Here for More Information](#)



If you have any feedback, or if you feel that you have received this in error, please e-mail michaeltaylor@chesleybrown.com or call (770) 436-3097