COVERING ALL FORMS OF WORKPLACE PROTECTION
IN TODAY'S ENVIRONMENT

ioma
Business Intelligence at Work

SECURITY DIRECTOR'S REPORT

ISSUE 08-12 WWW.IOMA.COM/SECURE DECEMBER 2008

SDR SURVEY

What Are the Best Ways to Get Top Management to See Security's Value?

Your security operation can strive to be world class, but it will never be as effective or efficient as it can be if top management doesn't see the good in it. Studies prove that management's recognition of security's strategic importance precedes the budget you need to do the job. Without it you'll have to scrape by—and even that's not a sure thing in these tightfisted times. So how do you get management to see the light?

It's a question that is sure to hit home with a majority of security executives. According to the results of a new survey by *SDR*—of security leaders at

CONTINUED ON PAGE 11

New Data Reveal True Picture of Workplace Violence

By the most tragic measure—employee fatalities—violence has become a relatively less important issue of workplace safety. While the total number of annual workplace deaths due to other causes is a touch higher today than it was in 1992, the number of workplace homicides has been cut in half. And workplace assaults comprise less than 4 percent of all lost work-time injuries and illnesses. But statistics sometimes can paint a false picture of the position that violence prevention should have within the overall workplace safety program.

CONTINUED ON PAGE 13

CRISIS RESPONSE

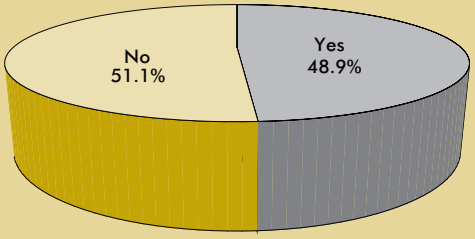
Alert Planning Should Factor in Messaging Limits

Most students at the University of Southern California (USC) have registered with TrojansAlert, the school's emergency notification system, to immediately receive a text alert in the event of a campus emergency. So after a student was recently stabbed and killed, several registered students who didn't get the alert and heard about the incident secondhand,

CONTINUED ON PAGE 14

ALSO IN THIS ISSUE

Is the Strategic Value of Your Security Department Adequately Recognized?.....see top story



(Source: *SDR*)

Q&A

Will Your People and Property Be Safe During an Evacuation?

The mass evacuations that preceded Hurricanes Gustav and Ike got us wondering exactly how security departments should prepare to protect property in such an event. So we asked one of the most knowledgeable people we know, Michael Blyth, director of risk consulting for British Security Group, LLC (www.thebritishsecuritygroup.com).

Blyth has an impressive history of global security experience, and few are as expert in the area of crisis management as he is. He is also the author of an excellent resource, *Security and Risk Management: Protecting People and Sites Worldwide* (Wiley, ISBN: 978-0-470-37305-7), and has a second book being published in December titled *Business Continuity Management: Building an Effective Incident Management Plan*. The following are some of his thoughts:

. . . On leaving people behind. Of course the nature of the operating region and the circumstances for evacuation will determine whether a stay-behind party will be used to protect facilities or materials during an evacuation. When determining who to leave behind in foreign locations, companies may choose to use local security elements that might not be subject to the same risks as expatriate security personnel if events such as civil disturbances or political instabilities precipitate the evacuation. Threats faced to local personnel should always be carefully considered as well. If the cause of the evacuation affects everyone, such as a natural disaster or pandemic, then a company may choose to close down and secure a location rather than place any security personnel at risk.

For domestic evacuations triggered by civil disorder or natural disasters, there must be a careful balancing of risks to staff and the protection of a facility, and choices to leave a security detachment in place reflect whether the security staff would be safe and could be sustained during the crisis. But typically when an evacuation decision is made, organizations withdraw all staff from a site because the circumstances present risks to both security personnel and company staff.

. . . On making the call. If companies are considering leaving a security element behind to secure their facility, there are a number of factors to think about when deciding which management and security elements should remain. First, companies should consider the risks faced by those security personnel: Can they be protected or protect themselves from the risks that have triggered the evacuation? Hurricane

Managing Editor: DAVID SOLOMON
Desktop Editor: HILARY SLOIN
Sr. Marketing Manager: LARAINE KELLY

Editor: GARETT SEIVOLD
Research Manager: BIKRAM GAUTAM

Sr. Managing Editor: JANICE PRESCOTT
V.P., Publisher: RANDY COCHRAN
President: JOE BREMNER

SECURITY DIRECTOR'S REPORT (ISSN 1521-916X) is published monthly for $419 per year by the Institute of Management and Administration, Inc., 1 Washington Park, Suite 1300, Newark, NJ 07102-3130. Periodicals postage paid at Newark, NJ and additional mailing offices. POSTMASTER: Send address changes to *SECURITY DIRECTOR'S REPORT*, 1 Washington Park, Suite 1300, Newark, NJ 07102-3130; 973-718-4700; fax: 973-622-0595; e-mail: subserve@ioma.com.

Katrina also made it clear that risks faced by security personnel's families are a conflicting consideration—will security personnel be motivated to help their own families move to safety and be unavailable or unreliable in terms of remaining to protect the company's interests?

Another basic consideration is whether security personnel can be sustained in terms of power, utilities, and life support. Companies should put in place resources to avoid creating a situation in which another group needs to be evacuated because it has run out of water or food while securing a site. Finally, companies should consider whether the security group can bring real value by remaining on-site—can they protect the facility under any restricted conditions that might result from the crisis event? Creating a comprehensive evacuation management plan, which supports the facility security plan, will help a company understand what limitations may result during an evacuation scenario and what resources and decision paths need to be developed before a crisis occurs.

. . . On protecting those left behind to protect facilities. Companies have a moral and of course legal obligation to protect their security staff to the same levels as they would other staff. Companies should therefore ensure that any security personnel appointed to protect a facility during an evacuation have the tools, training, and support required to deal with threats and challenges that might arise. In addition, a stay-behind party doesn't operate in isolation. It should have the support of the company or government agencies in terms of resources and information.

That said, often circumstances will require the group to be self-sufficient for periods of time due to the likely effects on normal communication media, transportation lines, and basic utilities. The company can best protect any security personnel left behind by developing a clear and pragmatic understanding of what that group is expected to achieve and aligning resources so it can accomplish those objectives. This may mean that the security personnel don't protect the entire facility, just critical structures to reduce their geographic risk exposure.

In addition, a contingency planning approach should include having robust communication systems in place, with the ability to call upon government support agencies should the security group face challenges that overwhelm it. Members of the security group should understand clearly how to call on predefined help if they find themselves in trouble. Planning and preparation is fundamental for stay-behind parties to be both safe and effective.

. . . On getting police to watch your stuff. Companies should exploit local government relationships and capabilities in advance of a crisis. Develop crisis-management plans in alignment with local

How Well Will You Handle an Evacuation?

Crisis management expert Michael Blyth, British Security Group, suggested asking five basic questions for an indication if you have a little more work to do to prepare for an evacuation crisis:

1. Do you understand the threats and challenges at the strategic, operational, and tactical levels you will face?

2. Have you drawn upon all available knowledge, capabilities, and resources—both in-house and from government and other commercial groups—to best manage a crisis?

3. Do you have a defined and tested crisis management organization, and have you considered the value of special response teams in dealing with a crisis?

4. Do you have clear, transparent, and tested crisis-management policies and plans in place that adequately protect people, facilities, and assets?

5. Does your company have the ability to sustain a site independently of local utilities and continue communications if public systems fail?

Even more fundamentally, the question a company should ask itself is: If a crisis occurs, do you think everyone will have a good idea of what they or their groups will do, and can they do it effectively and safely?

authorities to draw upon their significant resources and capabilities. Often during the initial stages of a crisis, local authorities will struggle to deal with the widespread and urgent needs of the commercial and public sector. However, once some form of stabilization occurs, those companies with integrated policies and plans will stand a better chance of receiving critical support from local authorities. Companies should seek to develop collaborative crisis-management plans with local authorities in terms of leveraging information, knowledge, experience, and resources.

. . . On fortifying left-behind facilities. A loss of social order can make it very difficult for companies to prevent saboteurs or looters from damaging or stealing property. Fences and gates are largely a psychological barrier and can be scaled or breached easily without some form of human response mechanisms in place to intercept intruders. Locks and doors can often be forced, and alarm systems are only as good as the ability for local law enforcement or the company's security team to respond. Companies can, however, create a critical materials register—whether critical materials are information, structures, or materials—and develop plans to either evacuate critical materials with their departing project team (laptops, documents and files, or portable assets) or move materials to a hardened facility that has better security (high-value materials or vehicles). Strengthening critical structures might also be an option if the company is concerned that any damages may have a catastrophic effect upon the organization.

. . . On getting back in before the average Joe. As part of contingency planning with local authorities, companies can seek to establish agreements that reflect their unique requirements in terms of having personnel return to the facility while the area may still be off limits to the general public. Trying to gain such permissions while a crisis is still occurring or while local authorities are still dealing with the effects will be difficult if not impossible. If predefined agreements are already in place, the company will stand a better chance of gaining both agreement and support from local authorities.

. . . On common evacuation planning mistakes. Companies often make mundane mistakes, such as spoiled food, fires resulting from appliances being left running, or IT issues resulting from power spikes or weather damage. Errors can also be unique, such as having to deploy special security teams comprised of armed personnel to return to a facility while the crisis is still under way to retrieve critical information or materials unintentionally left behind. The main error is failing to know when to evacuate and not having predefined policies and plans in place. All other errors flow from this key point.

If companies have predefined mechanisms for identifying a threat and triggering a proactive evacuation, then they will significantly reduce the potential risks faced to the facility and organization as a whole.

. . . On helpful technology. There are some useful technologies that can support companies evacuating facilities and perhaps leaving security personnel in place. Communication media that don't rely on local systems, which frequently fail, allow information to flow between those who stay behind and supporting corporate and government groups. Portable CCTV systems can allow corporate or other parties to view the local conditions or damages and threats to their facility remotely—and respond in a more informed manner. Any technology that helps secure assets, allows managers to better understand the situation, and relates accurate and timely information allows for better crisis management. ❑

Online Investigations Can Reveal Unknown Threats

In recent months, two employees at the University of New Mexico Hospital used their cell phones to take close-up pictures of emergency room patients' wounds and posted them on a MySpace page. The hospital learned of the privacy and policy breach thanks to an anonymous tip, and it promptly fired the two employees and disciplined other workers who knew about the violation but failed to report it. According to experts, this is just one type of troubling security breach that an investigation of social Web sites can reveal.

Mining MySpace, Facebook, and similar sites can yield unknown threats, according to author and expert Cynthia Hetherington (*Business Background Investigations*) during a presentation on Web investigations at the annual conference of ASIS International. She advised security executives to search MySpace for their company name to see what it returns. Many instances will be harmless job listings, but a search can also yield employees who are revealing more about the work they do than your company wants—potentially even sensitive information. Less serious but still problematic are employees whose MySpace activities tarnish or reflect poorly on the company's reputation or brand.

Potential hires are also fair game, said Hetherington, who noted a trick to reading people's profiles that are set to "private." Take the numbers that appear at the end of the URL for a MySpace page of interest and do a Google search on it. These numbers are, essentially, a MySpace user's Social Security number, and a Web search can yield cached versions of the page before it was set to private. (Note: While a MySpace investigation of job candidates may be legal, there are important steps to take to avoid legal challenges detailed in the accompanying sidebar.)

The "MySpace Visualizer" on Lococitato (www.lococitato.com) is a tool for uncovering links between MySpace users, potentially helpful in an investigation where you are looking for a connection between a certain supplier and employee, for example. A similar tool is being developed for Linkedin (www.linkedin.com), which may become extremely useful in creating a picture of relationships during workplace investigations.

Lococitato and Yoname (yoname.com) are probably the most useful Web 2.0 investigation tools, according to Hetherington. Yoname searches social Web sites and provides investigators with an individual's

Security Calendar

Executive Protection/Security Force Management, New Orleans, Dec. 8-12. Contact: ASIS International, 703-519-6200; Web: www.asisonline.org

Wharton/ASIS Program for Security Executives, Philadelphia, Feb. 2-6, 2009. Contact: Customer Care and Program Consultation, 800-255-3932; Web: http://executiveeducation.wharton.upenn.edu

ASIS International 3rd Asia-Pacific Security Conference, Hong Kong, Feb. 3-5, 2009. Contact: ASIS International, 703-519-6200; Web: www.asisonline.org

IAHSS Midwinter Conference, Las Vegas, Feb. 8-10, 2009. Contact: International Association for Healthcare Security & Safety, 888-353-0990; Web: www.iahss.org

SecurePharma 2009, Philadelphia, Feb. 23-25, 2009. Contact: WBR, 888-482-6012; Web: www.wbresearch.com/securepharmausa.com

Homeland Security 2009, Washington, D.C., Feb. 25-26, 2009. AFCEA International, 703-631-6236; Web: www.afcea.org/events/homeland

Before You Search MySpace for the Dirt on That Next Job Applicant

It's now routine to conduct Internet searches on job candidates, but they can expose employers to legal challenges ranging from privacy invasion to discrimination, cautions attorney Lester Rosen of Employment Screening Resources.

He said trolling the Internet—via Google, MySpace, Facebook, blogs, chat rooms, online forums, YouTube, and so on—is attractive for employers because it can turn up a "treasure trove of applicant information" and allows to "look under the hood" at potential hires, said Rosen. However, Internet searches are "not as easy as you think just because you have a browser and a mouse," Rosen said during a recent Webinar hosted by the Bureau of National Affairs.

The law is still developing in this area for both sourcing and screening candidates, and very few cases are exactly on point. Rosen suggests a few things to consider about such investigations:

- Using search engines to investigate job candidates is low risk. Deeper digs into social networking sites can raise the potential for privacy invasion, especially if the candidate's site is password protected.
- Using a pretext or fabricating an identity to penetrate a candidate's social network is even riskier. Such a tactic is "pretty clearly where an employer would get in trouble," Rosen said.
- Legal considerations in this area include a candidate's reasonable expectation of privacy, the employer's potential intrusion of seclusion, as well as violation of the Internet sites' privacy policies and terms of use. (Most states have passed privacy laws or have developed common law privacy rights that social networking site investigations could violate.)
- What if you discover protected information about a candidate during a search—such as the candidate's age, ethnicity, or sexual orientation? Rosen said it is tough to "unring the bell" and prove that the information did not affect an employment decision so as to avoid charges of prohibited discrimination. "It's a hard road to claim you disregarded information found on the Internet," said Rosen.
- Information on the Internet may not be accurate or may apply to an individual who merely has the same name as the job candidate. Not only is the potential for malicious manipulation of identities on the Web real, but people may be doing "a little bit of 'puffing' or just having a little fun," he said.

Advice: The most conservative approach is to obtain the candidate's consent for an Internet search after the employer has made a conditional job offer, Rosen said. "Consent cures a lot of ills." Although he warned that even with consent, the employer has to be careful not to make employment decisions based on a candidate's membership in a protected class. "No one under law can consent to being discriminated against." (Also, the federal Fair Credit Reporting Act requires employee consent to any background checks performed by third parties, which would also apply to third-party Internet background investigations.)

Federal case law indicates that an employer can refuse to hire a candidate who declines consent to an Internet background search, especially if the search is part of a standard hiring procedure embodied in a written policy that affects all applicants, said Rosen.

username, which he or she likely uses in many forums and can often provide a shortcut in workplace investigations. For example, by searching eBay for the username moniker of a suspected insider thief, you could quickly confirm your suspicions upon discovering he is auctioning company property.

Social Web sites can also introduce unintended risks, especially to key employees and top executives. It's not uncommon to find researchers who reveal enough bits and pieces about themselves and their work to make themselves and confidential company information more vulnerable. The recent hacking of Sarah Palin's private Yahoo e-mail account highlights the possible danger from personal details floating around in cyberspace. A hacker reportedly reset the vice-presidential nominee's password by conducting simple Google searches to answer security questions such as, "What was your high school?" "You also need to check Linkedin profiles of company executives to make sure they're not overexposing themselves," said Hetherington.

Finally, Hetherington sees the 3D virtual world of SecondLife (www.secondlife.com) becoming a more important element in an effective Web investigation strategy as it grows in popularity and is increasingly used as a tool for both conducting work and criminal activity (hacking and money laundering, for example). "Start looking into SecondLife now to stay on top of [having an effective Web investigation strategy]," she advised.

More information. MySpace is only one of several Web sites that security departments should routinely mine as part of background, due diligence, and theft investigations. Visit the list of *SDR*'s supplemental materials online to link to the most valuable sites (www.ioma.com/corporate_security). ❑

DATA SECURITY

Lawmakers Begin to Catch Up to Corporate Data Security Failures

It has been another record-breaking year for corporate reports of data breaches—taking companies only eight months to surpass 2007's total—and all companies are now faced with having to pay for past security failures. Lawmakers are imposing new rules and regulations for information protection, effectively changing the return on investment for data protection measures that many companies have so far resisted.

More regulation was inevitable. In addition to data breach reports reaching an unprecedented level, it's well-known they represent a fraction of total incidents. Surveyed at the RSA conference in August, 300 data security professionals indicated that up to 89 percent of incidents go unreported. It happens so frequently that only 8 percent of Americans are "very confident" institutions can house their personal information securely, according to a national survey conducted by The Strategic Counsel.

FTC red flag rule. One of the most wide-reaching yet somewhat ambiguous of these is new identity theft prevention rules enforced by the Federal Trade Commission. Under the rules, which became effective Nov. 1, financial institutions and "creditors" must develop prevention programs that identify relevant patterns, practices, and specific activities that are "red flags" for possible identity theft.

Although the deadline to comply has come and gone, it's still unclear to many exactly who the rule covers. "One of the most frequently asked questions is whether or not they're covered by the rules at all," said Pavneet B. Singh, FTC Division of Privacy and Identity Protection. The "creditor" category includes a diverse mix of industries that come under the FTC's jurisdiction, including finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications firms. Kevin Lyles, a partner in the Columbus, Ohio office of Jones Day, said the creditor category is huge and includes retailers. And experts generally agree that hospitals may well be covered by the new rules if they set up patient accounts to collect regular payments—something nearly every hospital does. "It's any business that issues credit to its customers, so if you allow customers to defer payment for any goods or services, you're a creditor, and you're covered," said David Medine, an attorney with Wilmer Hale.

Singh said the commission was still working out a rules enforcement strategy, and the FTC is also late delivering a promised guidance document. Because of the delay, experts believe it will be some time before the FTC enters "gotcha" mode. Singh acknowledged as much, saying that the FTC generally looks for good-faith compliance efforts for a period of time after a rule becomes effective.

As for complying with the new requirements, which amend the Fair and Accurate Credit Transactions (FACT) Act of 2003, the key is to develop a program that identifies the red flags that signal possible identity theft, as well as how the organization would respond to prevent or mitigate identity theft, said Singh. In addition, the program must be updated periodically to reflect changing identity theft risks. However, the rule leaves many implementation details up to individual organizations because of the different industries that fall under it.

CONTINUED ON PAGE 10

NEWS BRIEFS

WORKERS' CIRCUMVENTING IT SECURITY PUTTING COMPANY DATA AT RISK

According to a global survey by Cisco Systems of more than 1,000 end users and 1,000 IT professionals, employees are taking risks—such as altering security settings and installing unauthorized applications and programs—that can lead to data losses. Overall, 67 percent of workers have engaged in one or more activities that threaten corporate security on some level. Some of the more common:

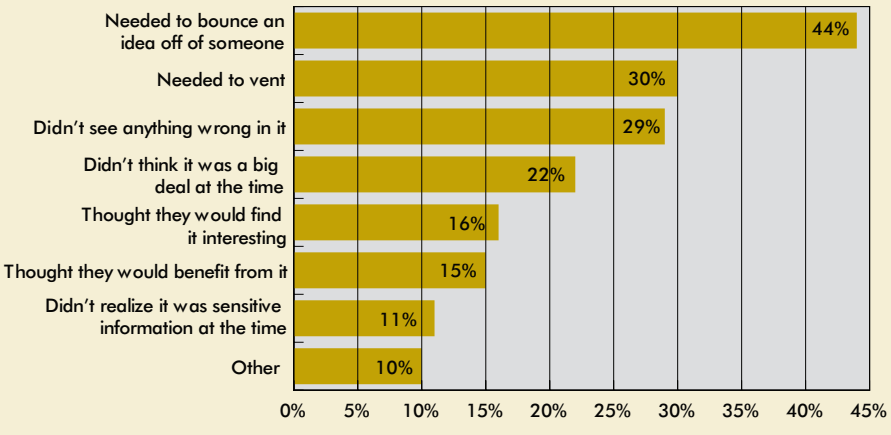
- Stepping away from a computer at work without logging off or shutting down, 37 percent;
- Storing computer password and login information on their computers at work, 19 percent; and
- Throwing unshredded corporate paperwork into the garbage, 18 percent.

Complicating matters is the move by companies—for reasons of cost and efficiency—to issue more laptops, which 78 percent of workers say they also use for personal computing. More than four in 10 have allowed someone else, such as family members, friends, or co-workers, to use their company-issued laptop without supervision.

Although risk-taking behavior is global, the differences in employee behavior that the survey found suggests that "one size doesn't fit all" with regard to security policies, according to Fred Kost, director of security solutions at Cisco. "You may have to have different policies in different parts of the world," he told us—and not only to account for cultural differences but legal and regulatory constraints as well.

Another lesson is to remove to the full extent possible the ability of employees to change security settings, something 14 percent of employees admit to for reasons such as "no one will know" and "it's not my company's business which Web sites I visit." Lastly, companies still have some work to do to get employees to closely protect sensitive information about their job. Some 16 percent of U.S. workers admit to such improper disclosures with acquaintances and 2 percent with strangers.

Employees' Reasons for Sharing Sensitive Work Information With Others



(Source: InsightExpress/Cisco)

THREE KEYS TO GOOD INTERNATIONAL ADVANCED WORK

International personnel protection was a focal point of the recent conference on corporate and homeland security at California University of Pennsylvania, including executive safety. On the issue of advanced work items that security teams must concentrate on, the team leader for executive protection for Limited Brands suggested

NEWS BRIEFS

the availability and quality of local medical assistance and good communication with a strong network of local contacts. Also, an understanding of local culture. Without it, it's impossible for agents performing close protection to differentiate a legitimate threat from a regional or local custom.

TERRORISM INSURANCE DEEMED REASONABLE BUT MANY FIRMS DON'T HAVE IT

More than seven years after the 9/11 terrorist attacks, where are we with terrorism insurance?

- Approximately 40 percent of very large U. S. companies don't have it, according to terrorism insurance expert Erwann Michel-Kerjan from the Wharton School of Business's Risk Management and Decision Processes Center.

- Certain commercial property policyholders, particularly those that "own large, high-value properties in areas where many large buildings are clustered, particularly in urban areas viewed as a high risk of attack" still face problems finding terrorism coverage at prices or limits they consider reasonable, according to findings reported by the Government Accountability Office to a congressional committee.

- Overall, however, "commercial property terrorism insurance coverage appears to be available nationwide at rates policyholders view as reasonable," according to the GAO. In fact, Michel-Kerjan thinks terrorism coverage is probably underpriced in the United States, noting in a recent interview that the cost of coverage is up to four times as expensive in Germany for properties with similar exposure.

PREVENTING AND HANDLING EMPLOYEES' ETHICAL LAPSES

Mike Kotlatski, security manager for the City of Seattle, believes companies should manage a major fraud, scandal, or ethical lapse in the same way they address a hurricane. "I believe that the response to ethical lapses should be part of the business continuity or disaster recovery plan," he said in an address to the 2008 annual conference of ASIS International. For one thing, it betters the odds that the company will speak to the issue with one voice, which is particularly critical in cases of misconduct. "You need a single point of contact who speaks to the press, tells them an investigation is under way, who is doing it and what the timeline is, and when you hope to have the results." By getting out in front of the story in a coordinated manner, companies can minimize press speculation, he suggested.

As for prevention, Kotlaski says that companies can't shield employees from ethical quandaries nor command their choices via ethics policies—noting that Enron had a "nicely written ethics policy." What should security leaders be doing? "In the end, it will be up to the individual what actually happens and it's our job to identify and give them the tools to make the right choice." He believes it is often the other way around. "We tend to look at people who do things wrong and correct them instead of giving people the tools to do things the right way the first time." Leading by example is an important part of improving the department and company culture, he said, as is getting to understand the people you supervise. "If you take the time to get to know people, you can notice when things are wrong and prevent people from making missteps."

Data Security Failures

CONTINUED FROM PAGE 7

For the many organizations that already have various policies and procedures for preventing identity theft, the real compliance burden is establishing a single, written program that has senior-level approval, Lyles said, and this is the real goal of the new rule, according to Medine. "The idea was to escalate this to the highest levels of the company." While the rules do not provide a private right of action to allow individuals to file lawsuits or set criminal penalties, they do allow the government to seek civil penalties.

The game-changer in Massachusetts. It's not only the FTC that is trying to put the brakes on identity theft. Massachusetts has implemented sweeping new security regulations, which take effect Jan. 1, 2009, requiring companies to encrypt on laptops personal information such as credit card account and Social Security numbers when they are stored with an individual's name. Michigan and Washington state are considering similar regulations. And a Nevada law took effect in October that requires businesses in the state to encrypt personally identifiable customer data, including names and credit card numbers, when they are transmitted electronically.

Companies need to assess their compliance against this new wave of regulation in each state in which they operate, but what is the bigger trend? How can companies get in front of regulators and the new patchwork of regulations? Thomas Smedinghoff and Laura Hamady, in the privacy and data security law practice of Wildman Harrold, see movements in the state, especially the new Massachusetts law, as evidence of the accelerating development of two key legal trends: (1) the expanding scope of the duty imposed on companies to provide reasonable security for their data and (2) the growing reliance on requirements for the use of encryption in certain cases.

The new Massachusetts standards apply to "all persons that own, license, store, or maintain personal information about a resident," which means it's likely to have a nationwide impact similar to that of California's pioneering breach notification law and may inspire other states to adopt similar legislation, according to the attorneys. They also constitute one of the most comprehensive sets of general security regulation yet seen at the state level. "At the same time, however, these regulations are clearly modeled after aspects of developing data security law at the federal level, making them perhaps a logical next step in the continuing expansion of corporate security obligations," write the attorneys ("New State Regulations Signal Significant Expansion of Corporate Data Security Obligations").

Like the law in at least nine other states—Arkansas, California, Connecticut, Maryland, Nevada, Rhode Island, Oregon, Texas, and Utah—the Massachusetts regulations are intended to protect the "security and confidentiality" of personal information about residents. But unlike those other state laws, which merely obligate companies to provide "reasonable security" to achieve that goal, these require companies to:

- Implement a risk-based, process-oriented, "comprehensive, written information security program" in accordance with a detailed list of requirements; and

- Encrypt all personal information stored on laptops or other portable devices, all records and files transmitted over public networks "to the extent technically feasible," and all data transmitted wirelessly.

Smedinghoff and Hamady say that by adopting the regulations, Massachusetts

has, in effect, become the first state to formalize the definition of "reasonable security" under those laws. The Massachusetts regulations, like FTC policy and Oregon that also require a comprehensive security program, specify certain physical security controls that a covered company must address (as well as administrative and technical controls): reasonable restrictions on physical access to records and storage of such records and data in locked facilities, storage areas, or containers.

The Massachusetts regulations also mark an important departure from a solely risk-based approach by imposing obligations to use encryption in certain situations regardless of the presence or absence of otherwise reasonable security.

According to Smedinghoff and Hamady, the new regulation is a game-changer. "The borderless nature of modern electronic commerce may well make the Massachusetts regulations de facto law of the land for many companies. If a company is not currently subject to a legal obligation to develop and implement a comprehensive written information security program, it likely will be soon." Some of the requirements companies may not find burdensome, say the attorneys, but others, such as aspects of the employee training requirements, may be.

New rules for defense contractors. Finally, under a proposed rule issued by the Defense Department Oct. 9, Defense Contract Management Agency contractors operating or maintaining systems storing nonpublic and sensitive private information would have to sign a nondisclosure agreement acknowledging responsibility for the safeguarding of such information. Contractors, under the policy, would need to protect the improper release of personally identifiable information "to the maximum extent practicable." ❑

Security's Value

CONTINUED FROM PAGE 1

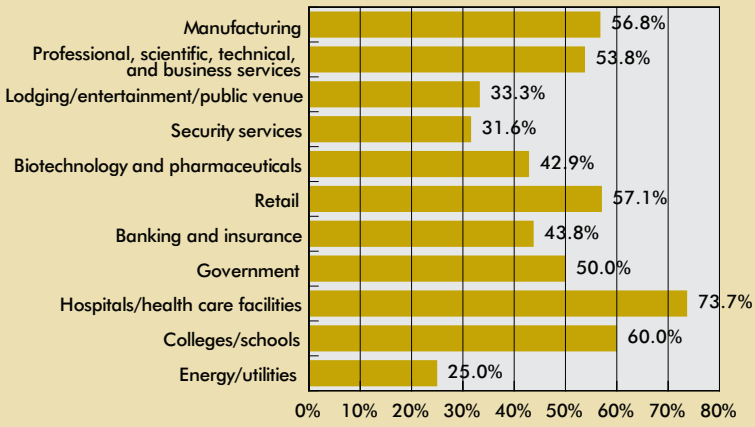
275 organizations—a troubling 51 percent think the real value of physical security is not adequately recognized (see the figure on page 1).

In some industries, security seems to be getting more of its due, such as in the energy and utility sector, but in many it is distressingly low. Three out of four hospital security directors think security's actual value goes unappreciated (see Figure 1). Even at billion-dollar companies, appreciation for security is hit-and-miss, according to the results. Exactly half of all CSOs at large corporations said their firm doesn't understand security's value.

It is certainly troubling that security has yet to earn full recognition for what it actually is—the foundation upon which all business opportunity rests. But the survey results show that it is achievable—and that a system for measuring performance can help security departments reach the goal.

Security departments with a formal performance measurement system in place—one that sets acceptable or baseline performance levels, sets targets for improvement, and tracks performance relative to

Figure 1. Inadequate Recognition of the Physical Security Department's Strategic Value by Industry



(Source: *SDR*)

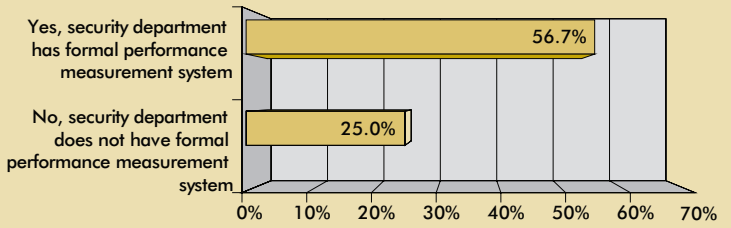
goals on a continual basis—are more than twice as likely than those without a system to have security's strategic value recognized (see Figure 2). Performance measures and return-on-investment calculations, by casting security in business terms, are effective ways to encourage management to adopt a permanent, strategic view of security, in addition to creating an effective channel for sharing information about security risks with senior management.

The ability for security performance measures to communicate value is something security executives seem to intuitively understand. The survey asked security executives how much sway they think different methods have in communicating security's value to management, and a metrics program ranked second overall. (It rated 3.6 on a 1-to-5, not-effective-to-extremely-effective scale.)

What came in at number 1? One-on-one meetings. Personal interaction between security and company leaders is thought by security professionals to be the most effective way in which to communicate the value of security, according to the survey. Personal meetings rated number one among respondents at all size companies and are seen as especially effective by security executives at large companies (see Figure 3).

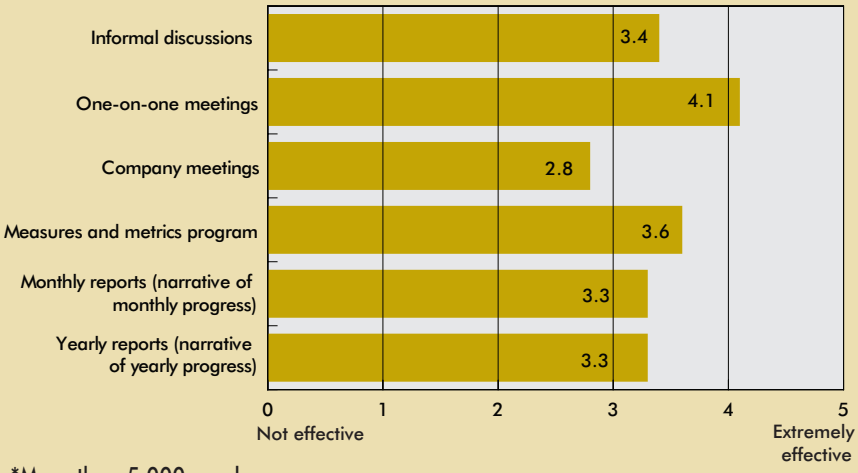
For more information. Complete data from IOMA's survey will be available in a forthcoming publication, *Physical Security Performance Measures, Benchmarks & ROI Report, 2009*. Based on analysis of 275 security departments, the report examines how companies measure physical security performance, including what sources of information they use for performance data and how security departments make use of them. It also reports on more than a dozen specific measures of physical security performance, such as the percentage of false alarms and laptop theft rates, and the level of performance that is normal in each area. Finally, the report examines the process that companies have for demonstrating the value of the security department and for making a business case for security expenditures, including norms in reporting to management and the use of various financial metrics to demonstrate the worthiness of proposed security investments. Visit www.ioma.com and select the Corporate Safety & Security Focus Area for this and all security benchmark research. ❑

Figure 2. Effect of Performance Measurement on Recognition of Security's Strategic Value



(Source: *SDR*)

Figure 3. At Large Companies*, How Effective Are Different Methods for Communicating Security's Value to Senior Management?



*More than 5,000 employees

(Source: *SDR*)

Workplace Violence

CONTINUED FROM PAGE 1

A more complete picture. It's true that the number of workplace homicides is way down and that assaults account for less lost work time than most all other injury and illness categories—including repetitive motion injuries, falls, slips, and overexertion. But if companies focus on the raw numbers to guide their workplace safety priorities, they may be making a costly error. Examples:

- Companies are making better progress against other causes of injuries. There has been a decline in both workplace assaults and total workplace injuries since 1992, but there has been a larger drop in injuries overall than for assaults due to violent incidents, according to data by the Bureau of Labor Statistics. While the rate of all injuries has dropped consistently at about 5 percent per year, the overall decline for injuries due to violent incidents has not been nearly as significant, and the rate has even gone up almost every other year, including 10 percent in 2006 (see the accompanying figure).

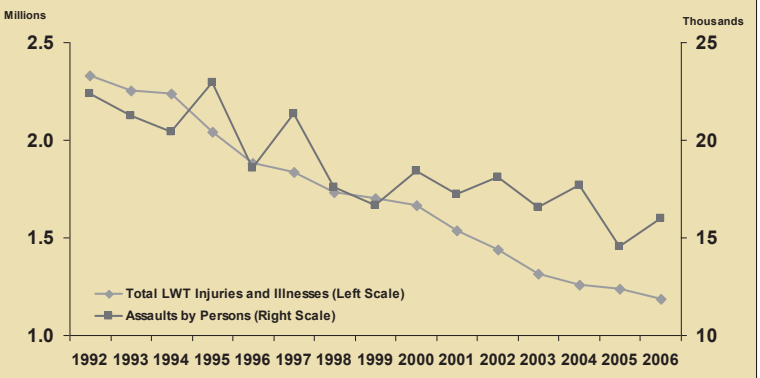
It's clear from the data that gains made in the prevention of workplace injuries from other causes are the result of permanent safety improvements, such as safer equipment or safer work processes, while reductions in workplace assaults are alterable and subject to swings in the general crime environment and workplace hostilities.

- Assault-related injuries are relatively more important as a workers' compensation matter. Claims related to crime-related injuries typically cost much more than injuries from other types. New data publicized by the National Council on Compensation Insurance Inc. (www.ncci.com), the nation's largest provider of workers' compensation data, shows that average payment in cases where injuries result from acts of crime is $11,381, compared to the overall average of just over $9,000. Only motor vehicle claims cost more on average ($13,2467 per claim).

Medical payments also tend to be higher when crime is the cause of the injury—$13,882 compared to $11,417 overall. Only burns and motor vehicle accidents result in higher medical payouts ("Violence in the Workplace—An Updated Analysis NCCI Research Brief," 2008).

- Prevention is increasingly a focus of regulation. Workplace violence can slide down the scale of safety priorities due to the fact that, unlike many other causes, there is no federal standard addressing it (it is only covered under the general duty clause that specifies that employers have an obligation to maintain a workplace free from recognized hazards). While this hasn't changed, states have started to target specific types of violence, especially in late-night retail establishments. And, most recently, New Mexico's governor signed an executive order mandating that its state agencies introduce workplace violence policies relating to the protection of victims of domestic violence and stalking.

Workplace Assaults Have Shown Less of a Decline Than Have Total Lost Work Time Injuries and Illnesses Since 1999



(Source: U.S. Bureau of Labor Statistics/NCCI Inc.)

It's important to treat workplace violence within the context of worker safety and not just as a security or human resources issue because it ensures that incidents travel the same rigorous accident investigations process as an injury caused by, say, a malfunctioning machine. This results in the safety committee conducting a root-cause analysis for every event, rather than merely an annual workplace violence audit, and also improves the odds of controls being put in place that do not specifically address HR or security concerns. For example, an OSHA investigation in 2007 of a psychiatric facility found that unsecured items were posing a real threat to workers, including television equipment, chairs, and tables. Treating violence prevention as an occupational safety issue also helps it take its rightful place alongside other workplace safety training topics. ❑

Messaging Limits

CONTINUED FROM PAGE 1

were vocal in their displeasure. The alert system did successfully push out thousands of alerts, but it wasn't seamless, and security executives and crisis teams shouldn't expect them to be, according to new research.

The promise. In September, the University of Arkansas launched and promoted their new emergency communication service—called RazALERT—that gives administrators the ability to send an alert within minutes to everyone in the campus community via phone and text messages (part of the Connect-ED communication service from Blackboard Connect Inc., www.blackboardconnect.com). The school is just the latest to roll out a new mass messaging system, and many more will follow now that a new measure has been signed into law that requires higher education institutions to develop systems to immediately notify students of a campus emergency. Some corporate campuses are also adopting these systems as a central piece in the company's emergency response plan.

The limitations. A professor at the Georgia Institute of Technology (GIT) has authored a new study that says—while cell networks represent a promising platform for dispersing alert messages—today's networks aren't exactly up to the task. "Through a series of experiments, we have shown that even under optimal conditions, these networks [whether through voice calls or text messages] cannot meet the 10-minute alert goal set forth by the public EAS [Emergency Alert Systems] charter."

The fundamental problem is that cellular networks are not designed for the delivery of emergency-scale traffic loads. So they simply cannot handle the influx and congestion that blocks the delivery of emergency alerts, according to the research. "Moreover, we have demonstrated that the extra text messaging traffic generated by third-party EAS will cause congestion in the network and may potentially block the delivery of critical information, such as calls between emergency responders or the public to 9-1-1 services." ("Characterizing the Limitations of Third-Party EAS Over Cellular Text Messaging Services," Patrick Traynor, Ph.D., September 2008.)

More mundane issues can also arise to create gaps in the alert system. In the USC incident, one reported cause for the nondelivery of alerts was that cell phone carriers' technology recognized the mass emergency alert as spam and didn't send it out—a bug the school is working out.

Scrap it? We certainly don't think that's the conclusion to reach. Cell phones are a terrific medium for distributing messages to people wherever they are, and efforts are under way to make networks more robust for handling emergency message loads.

But there is an element of hype to current third-party text messaging products, suggest researchers. "Many such services advertise text messaging as an instant, targeted disseminator capable of delivering critical information to tens of thousands of mobile phones when it is most needed." But those are inflated claims, according to testing. "Such services have been purchased by colleges, universities, and even municipalities hoping to protect the general public. Unfortunately, such systems will not work as advertised."

Universities and others attracted to the promise of this type of alert system need to recognize their limitations, and emergency planners should figure them into their overall emergency communication strategy. Testing systems and getting an actual handle on what they will and will not deliver in an emergency is also critical. Additionally, congestion isn't the only potential drawback that emergency planners must consider:

- Geographic targeting is currently difficult. So sending a text alert to mobile numbers on file for employees or for faculty and staff will deliver alerts to those individuals wherever they are, even if they are hundreds of miles from the danger. Conversely, this type of alert system isn't helpful for visitors or others who are on-site and in danger but who are not signed up to receive the alert. The GIT researchers view this drawback harshly. "Such services therefore fail to achieve the fundamental property required of EAS infrastructure—that all individuals with a device capable of receiving alerts can do so.

- Message authentication is impossible. As such, recipients need to trust the alerts they receive. However, it is possible for false text alerts to go out (and this has, in fact, occurred). "The implications of this limitation are significant. For instance, in the event of an emergency such as a chemical leak, it would be easy for a malicious party to send an 'all-clear' message before the situation was deemed safe. Because it would not be possible for users to verify the source of the information, maliciously induced confusion is a real threat."

- The order of message delivery isn't always predictable. The assumption is that text alert messages will be received in the order they are sent, something that emergency planners count on for providing continuity in instructions during the course of a crisis. However, the order that messages go out can be affected by a number of technical factors, and the effect can be troublesome, note the GIT researchers. The report quoted a Pepperdine University student who said messages during a wildfire evacuation created more confusion than clarity. "Each notification that was sent came through in six to eight text messages . . . And they were jumbled, not even coming in order."

The day may come when cellular networks can seamlessly handle mass notification and protocols being worked on right now are helping to move things in that direction, but it "will take time," the GIT report warns. Until then, emergency planners need to test systems for their actual capabilities, challenge vendors on their claims, and expect system weaknesses when creating an overall strategy for trying to get word out to stakeholders about an emergency situation. ❑

Coming in future issues of *SDR*

- What Is the Key to Identifying Persistent Security Weaknesses?
- Products of the Year—Winning New Devices to Simplify, Transform, and Galvanize
- How One Security Department Keeps Up With Its Company's Rapid Technology Adoption
- Corporations and Spies—What's the Threat and What's Just Myth?

SUBSCRIBE TODAY!

❑ YES! Please enter my subscription for the next 12 issues (including electronic access to all back issues) of *SECURITY DIRECTOR'S REPORT,* which entitles me to electronic access to the current issue section of www.ioma.com/issues/secure and all back issues of the newsletter, for $419 plus $16.95 s/h*.

❑ I'd like to save $168 on a two-year subscription for $670 plus $33.90 s/h.*

❑ YES! Send me *THE COMPLETE GUIDE TO PREVENTING VIOLENCE IN THE WORKPLACE* for just $299 plus $14.95 shipping/handling. (1122C).

❍ Enclosed is my check for $_____.

❍ Bill me/my company.

❍ Charge my: __Visa __MasterCard __AMEX

Card #: Exp.

Signature:

Tel.: ❍Home ❍Office

Name/Title

Company

Street

City State ZIP

E-mail

Copy and send to:

IOMA Subscription Department
1 Washington Park, Suite 1300
Newark, NJ 07102-3130

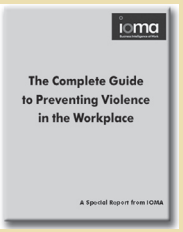
SDR 08-12

Phone: 973-718-4700 Fax: 973-622-0595

*By purchasing an individual subscription, you expressly agree not to reproduce or redistribute our content without permission, including by making the content available to nonsubscribers within your company or elsewhere.

From IOMA Research Reports

The Complete Guide to Preventing Violence in the Workplace



Year after year, security professionals identify workplace violence and bullying as their most significant security concern—greater than terrorism, Internet/intranet security, fraud, employee theft, and many others. Yet, many U.S. companies still remain complacent about dealing with workplace violence.

This exclusive report presents organizations with a specific, step-by-step plan for stopping workplace violence. In it, you'll find best practices from top experts around the country, including:

- Background on why a workplace violence plan is essential—and how it will save you money and increase productivity while reducing costly conflict and limiting your liability;
- Specific recommendations and a step-by-step plan for setting up a comprehensive violence prevention program in your organization; and
- Detailed administrative and proven security action items to prevent all forms of workplace violence.

Order your copy on the coupon to the left or call 973-718-4700 and ask for report #1122C. You pay just $299, plus $14.95 shipping/handling and your state's sales tax.

SECURITY DIRECTOR'S REPORT
1 Washington Park, Suite 1300
Newark, NJ 07102-3130

PERIODICALS