SDR
SECURITY DIRECTOR'S REPORT
March 2016 Issue 16.03 | Covering All Forms of Workplace Protection in Today's Environment | SDRmonthly.com

## ALSO IN THIS ISSUE



# Would You Know if You Had a Radicalizing Employee?

The risk that a terrorist could gain employment to carry out an attack has always been an issue of concern for U.S. critical infrastructure. The San Bernardino attack in December suggests that all organizations need to consider the possibility.

The threat is expected to be a hot topic at an ASIS Europe conference in London in April. "Given the impact of ISIL and their ideology, it is clear there is an increasing risk that organizations face when employees radicalize and become a potential terrorist threat," according to Werner Cooreman, head of security for DHL Express in Europe, who will be presenting at the conference ("Dealing with Insider Threat from Radicalization: "Employees Gone Rogue"). How to assess risk, detect insider threats, respond to suspicions, and report to authorities is "likely one of the bigger challenges of the coming decade," he believes.

continued on page 4

# Is Your Company's Hotline Serving Security's Goals?

In his 2016 audit plan for Springfield, Mo., Public Schools, auditor Wayland Mueller identified three areas of focus: payroll, building services, and athletics. His goal? Minimize fraud and waste. His tool of choice? A fraud and ethics hotline. Due to launch this month, Mueller expects to spend at least 10 percent of his time responding to crime tips and other reports made to the hotline.

It's probably a good idea, suggests results from biannual surveys by the Association of Certified Fraud Examiners. They typically find that tips are the most frequent way that organizations learn about fraud and theft.

**Trend.** The volume of calls to company hotlines is on the rise, according to recent

continued on page 10

# 5 Tips to Impress OSHA Compliance Officers

Early one morning in December, a man with a gun approached Susan Grant, a nurse at Texas Medical Center, in the employee parking lot. The assailant pistol-whipped her, knocking her down and chipping her teeth, and then made off with Grant's car. The incident is one type of assault that the Occupational Safety & Health Administration (OSHA) is trying to reduce by its focus on enforcing safety regulations that encompass workplace violence prevention in the healthcare sector.

Another type of incident—more common—is the assault of healthcare staff

continued on page 8

## Average Time to Detect System Breaches, 2014-2015.....see Briefs p. 6

| | 2014 | 2015 |
|---|---|---|
| Within the same day | 25.4% | 29.8% |
| 1 week or less | 24.4% | 36.8% |
| 1 month or less | 13.2% | 14.0% |
| 3 months or less | 2.4% | 3.5% |
| 5 months or less | 0.5% | 3.5% |
| 10 months or more | 1.0% | 0.6% |
| Unknown | 24.9% | 5.3% |

(Source: SANS Institute, Nov. 2015)

INVESTIGATIONS

# Polygraphs Deter Misbehavior But Can Also Spur a Lawsuit

The reputation of polygraph tests as a reliable method for detecting deception started to wane more than a decade ago after a National Research Council report suggested the technology is deeply flawed. Once considered highly accurate, most scientists now peg its ability to sort lies from truth at between 68 to 83 percent. Not great for a technology that carries significant legal risk (and when simple guessing is right 50 percent of the time).

However, in a 2012 internal review, the Dept. of Defense gave polygraphs some new life. A study concluded that polygraphs had resulted in nearly 4,000 admissions of misconduct during a 1-year study period. These ranged from security violations and failure to disclose foreign contacts to counterintelligence and criminal violations. The vast majority of admissions "would have gone undetected were it not for the polygraph process," the report concluded. The polygraph program also undoubtedly has deterrent value but it's difficult to measure, said researchers (*Office of the Under Secretary of Defense for Intelligence Department of Defense Polygraph Program Process and Compliance Study Report*, Northrop Grumman/TASC, Inc./Six3Systems, Inc., Dec. 19, 2011).

Recently, an experimental study took a crack at that last issue. Accuracy aside, does the prospect of a polygraph have the effect of making people more likely to adhere to security rules and regulations? (*Employees' Perceptions About the Deterrence Effect of Polygraph Examination Against Security Compromises*, Cook, 2015.)

The study gauged the impact of polygraph tests by surveying thousands of individuals who had and had not been subject to polygraph examinations within the past year. *The conclusion?* (1) Pre-employment polygraphs do not seem to significantly enhance adherence to security regulations by employees later. (2) But employees are significantly more likely to adhere to security regulations if a polygraph can be randomly administered at work.

"At the individual level, employees in sensitive positions who face random polygraph testing may take greater care to avoid even minor security infractions in order to avoid the possibility of a future deceptive reading on a polygraph test," according to the study. "Based on the findings, national security agencies should continue their enforcement of polygraph examinations that are required of certain security personnel."

## But not worth it?

Even if the prospect of a polygraph can tilt workers toward more honest behavior, using them can be risky.

Private sector employers generally can't require or request workers to take a lie detector test; can't take action against a worker for refusing to take one; and can't inquire about the results of a lie detector test given by another party. But there are exceptions. The Employee Polygraph Protection Act (EPPA) doesn't cover workers at government agencies or contractors working with government agencies. And the EPPA permits polygraph tests to be administered to certain job applicants of security service firms (armored car, alarm, and guard) and of pharmaceutical manufacturers, distributors, and dispensers. Also, subject to restrictions, the EPPA permits polygraph testing of employees suspected of involvement in a workplace that resulted in specific economic loss or injury to the employer (such as theft or embezzlement).

Attorney Lisa Guerin, author of *The Essential Guide to Workplace Investigations*, warns of the many legal hurdles to conducting tests legally. In workplace theft investigations, for example, you need to adhere to "a lengthy list of technical requirements." These include specific qualifications of the examiner, providing the employee extensive written notices before the test, including an exact list of all questions, and strict rules for conducting the test. You also need reasonable suspicion that the employee was

SDR
SECURITY DIRECTOR'S REPORT

**Garett Seivold** Editor
**Jack Trlica** Publisher
**Jim Lee** Executive Editor
**Kevin McMenimen** Chief Operating Officer
**Merek Bigelow** Director Of Marketing

SECURITY DIRECTOR'S REPORT (ISSN 1521-916X) is published monthly for $395 per year by Loss Prevention Magazine, Inc.  Periodicals postage paid at Charlotte, NC, and additional mailing offices. POSTMASTER: Send address changes to SECURITY DIRECTOR'S REPORT, PO Box 92558, Long Beach, CA 90809-2558; fax 714-226-9733; e-mail SDR@pfsmag.com. To renew, e-mail SDR@pfsmag.com.

involved in the theft, which includes having had access to the property that is the subject of the investigation. Finally, Guerin questions the utility of a polygraph test, noting that even if you follow all the rules, you still can't take action against a worker based solely on the test results.

**Recent legal cases.** Doctor John's, a chain-retail establishment in Midvale, Utah, recently learned the hard way about the intricacies of the EPPA. It lost a case brought by a former employee who was fired for refusing a polygraph test related to a theft investigation (a future trial will determine how much the company will need to pay). Although the company argued that it never really intended to administer an actual polygraph examination, the worker had surreptitiously recorded a district manager suggesting that if she was caught lying on the test that the case would be a 'slam dunk' for a local criminal prosecutor (*Amarosa v. Dr. John's Inc.*, D. Utah, No. 2-11-cv-676 DN, July 2, 2014).

In 2014, a former employee of a Premier Couples Superstore in Orlando, Amitra Alexander, filed a lawsuit after she was fired subsequent to failing a polygraph test as part of an investigation into $6,000 worth of missing lingerie. The shop owner allegedly subjected his 10 employees to polygraphs and only Alexander failed. She was then fired, but only for how she reacted to the news and not for the actual test result, the owner asserted.

While the case needs to play itself out in court (or settled in negotiation), it highlights why polygraph testing should be looked at warily by employers, according to analysis by the American Society of Employers ("Employee Fired Over "Failed" Polygraph Sues Employer," March 12, 2014). "Based on what is known of the case in question, the employer may need to explain how he could have "reasonably" suspected any of the 10 employees he tested if he had, as is alleged, told them they were not suspects. He may also have to explain how Alexander's behavior after she took the test—for which he allegedly fired her—had nothing to do with having taken the test."

It's also difficult to transfer liability in EPPA cases, as older case law shows (*Laney v. Getty*). In that case, an employer argued that since it had never even discussed the idea of a polygraph with the independent investigators it contracted to conduct a theft investigation, it shouldn't be held liable for the firm's missteps related to the EPPA. However, the EPPA broadly defines an employer as "any person acting directly or indirectly in the interest of an employer in relation to an employee or prospective employee." Because the contracted firm was acting on behalf of the employer, the company's attempt to evade liability was unsuccessful, according to attorney Ronald Miller (Wolters Kluwer). He warns companies to proceed with caution: "Even if an employer outsources the investigative function it would still be held liable for any violations of the EPPA based on the conduct of those individuals acting on its behalf." ■

## Security Calendar

- *RES/CON 2016 (formerly International Disaster Conference & Expo),* New Orleans, March 1-3. Contact: RES/CON General Information, 504-582-3072; Web: http://resconnola.com
- *13th Annual Campus Fire Safety, Security & Risk Management Conference*, Columbus, OH, March 7-8. Contact: Campus Fire Safety Com LLC and The Fire Code Academy, 800-771-3403; Web: www.campussafetyexpo.com
- *ASIS Assets Protection Course: Principles of Security (APC I)*, Indianapolis, March 7-10. Contact: ASIS International, 703-519-6200; Web: www.asisonline.org
- *Food Marketing Institute's 2016 Asset Protection Conference*, Tucson, AZ, March 14-17. Contact: Rhett Asher, 202-220-0774; Web: www.fmi.org/forms/meeting/Microsite/AP2016
- *First Defense Expo (FDX) 2016*, Louisville, KY, March 18-19. Contact: FDX, 770-912-6709; Web: www.firstdefenseexpo.com
- *Maritime Security 2016 East*, Norfolk, VA, March 21-23. Contact: Neak Media LLC, 203-221-2664; Web: http://maritimesecurityeast.com
- *Power Grid Resilience Summit*, Philadelphia, March 21-23. Contact: IQPC, 800-882-8684; Web: www.powergridresilience.com
- *ISC West*, Las Vegas, April 5-8. Contact: ISC West Client Services, 800-840-5602; Web: www.iscwest.com
- *ASIS International 15th European Security Conference & Exhibition*, London, April 6-8. Contact: ASIS International, 703-519-6200; Web: www.asisonline.org
- *Continuity Insights 2016 Management Conference: The Road to Resilience*, Nashville, TN, April 18-20. Contact: Advantage Business Media, 973-920-7789; Web: www.cimanagementconference.com
- *ASIS 26th New York City Security Conference & Expo*, New York City, April 27-28. Contact: ASIS International, 703-519-6200; Web: www.asisonline.org
- *Secure360*, St. Paul, MN, May 17-18. Contact: Susan Brauer, 612-374-6002; Web: http://secure360.org

## Would You Know if You Had a Radicalizing Employee?

continued from page 1

In response to the threat, it seems logical to increase the number of security personnel and conduct employee background checks. But when government facilities and companies reacted to the Sept. 11 attacks by dramatically increasing the hiring of security staff, a report for Congress on security staffing at critical infrastructures warned that the strategy also carries risk. "Expanding a guard force may increase opportunities for hostile "insiders" to infiltrate," it warned—noting that if 1 of every 50 security guards that an organization hires is a potential security threat, then the number of insider threats grows as it deploys more officers. And background screening, while clearly critical to reduce the insider threat, can't eliminate it, the report added (*Guarding America: Security Guards and U.S. Critical Infrastructure Protection*, Congressional Research Service, Nov. 2004).

In a July 2011 Dept. of Homeland Security (DHS) intelligence briefing, officials concluded that "we have high confidence…that insiders and their actions pose a significant threat to the infrastructure and information systems of U.S. facilities" and that "outsiders have attempted to solicit utility-sector employees" to commit attacks. DHS has long worried about such a possibility, highlighting it its *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. "The insider threat is becoming an increasingly serious concern for critical infrastructure," it warns—adding that terrorists have proven capable of conducting long-term clandestine operations, during which "individual members blend into daily life."

### What to do

Preventing against an insider attack is immensely complicated because of the significant advantage that insiders have compared to others who intend to harm an organization—a result of their authorized access and awareness of an organization's vulnerabilities, such as loosely enforced policies and procedures, or exploitable security measures. Indeed, the vast majority of security measures that organizations employ to defend against terrorism—hardening buildings, restricting access, implementing mail and delivery controls—do nothing to mitigate the harm that an employee or other authorized individual could inflict.

The Dept. of Defense (DOD) was tasked by Congress to get a handle on the insider threat facing its facilities following significant insider incidents in recent years. *Examples:* On Nov. 5, 2009, a lone Army officer shot and killed 13 people and wounded 32 others on base at Fort Hood, Texas. Almost 4 years later, on Sept. 16, 2013, a Navy contractor killed 12 civilian employees and contractors and wounded four others at the Washington Navy Yard.

Independent reviews of those and other incidents yielded numerous recommendations that DOD could take to protect against insider threats. In a recent audit of DOD's progress, the Government Accountability Office (GAO) cited examples of smart security actions that some facilities have taken as well as security gaps, including the failure to examine all policy and guidance documents through the prism of the insider threat (*Insider Threats: DOD Should Improve Information Sharing and Oversight to Protect U.S. Installations*, GAO, July 2015). Because the insider threat is not universally considered, policies did "not cover all DOD employees that could become either an insider threat or a victim of such a threat, did not identify multiple types of insider threat scenarios, or did not incorporate insider threats into their training requirements."

*Lesson:* To take action against the unique threat that insiders' pose, security directors should examine whether all security policies take the insider terrorist threat into account. *For example:*

- Policies that cover suspicious activity reporting should include examples of reportable employee behavior such as intimating support for a known or suspected terrorist organization.
- The counterterrorism program should include specific references to insider threats, assign responsibilities for the counterintelligence insider threat program, and identify procedures for processing threats from insiders believed to have relationships indicative of a potential threat.
- The workplace violence prevention policy (WVPP) should expand beyond workers on the payroll. The DOD's WVPP policy, for example, "does not apply to military and contractor personnel who could also become potential insider threats," warns the GAO audit. Anyone who has routine access to facilities and systems poses an insider risk, including contractors, temporary help, and lower-skill employees like cleaning personnel, and all should undergo thorough and periodic background screening.
- The insider threat should be incorporated into counterintelligence training requirements and antiterrorism awareness training. The GAO report says DOD needs to do a better job at both. "We found that the DOD Antiterrorism Standards, which was not updated after either the 2009 Fort Hood or 2013 Washington Navy Yard shootings, does not identify insider threats as one of the minimum antiterrorism awareness training requirements."
- Insider threat scenarios should be included within the emergency management response program. Although the DOD is updating its program, instructions for its emergency management program ignores "insider threat scenarios…such as the use of a vehicle-borne improvised explosive device or

a personal-borne improvised explosive device."

Vetting remains an important safeguard to avoid the recruitment potential terrorists, but companies can't rely on simple criminal background checks to reveal affiliations, warns terrorism expert Ty Fairman, president and CEO of ISAFE Group, an international security, logistics, investigations, and management company. He advises security teams at high-risk businesses to consider more detailed pre-employment interviews, to interview more individuals who know the candidate, and possibly even meet the individual in his or her home, to truly learn about an individual and not just the persona he or she presents at work.

But background checks alone are insufficient, warns Fairman, and Cooreman agrees: "It is a wholly different story when employees radicalize."

*What can you do?* Conducting surveillance of officers and other staff to spot suspicious behavior is important but terrorists are often experts at conscious assimilation and are not easily spotted by even the most mindful security operation, warns Fairman. Where infiltration is a threat, he advises companies to 'get personal' about employees and learn more about their home and social life. "Getting more personal knowledge about the workforce helps identify the conscious assimilator," he told *SDR*.

Dr. Park Dietz, founder of Threat Assessment Group, Inc., a provider of workplace violence prevention services for large organizations, said companies are at the very early stages of paying attention to radicalization as a phenomenon in the workplace but should cast a wide net when they do. "We're not looking only for obvious factors like Jihadist material or death threats, we're also looking for other kinds of misconduct ranging from the lowest level incivility and rudeness up to patterns of annoying and disrupting coworkers," he said (AirTalk, KPCC, Jan. 26, 2016).

A 3-year, $4 million European project called SAFIRE—Scientific Approach to Finding Indicators for & Responses to Radicalization—identified changes in a person's demeanor that—while not alone are proof of radicalization or intentions to commit extremist violence—may signal that a given person is in the process of radicalization (see the accompanying sidebar). "If a practitioner notices someone exhibiting a particular observable indicator, they can check the list of indicators to see if any more are relevant in order to help them decide whether to take further action," notes the SAFIRE report (*Observable Indicators of Possible Radicalization*, Sept. 2013).

Out of the 21 observable indicators, the five most frequently mentioned were:

1. Change in physical appearance/attire;
2. Disconnecting from former community;
3. Verbal expression against the government;
4. Expressed feelings of disconnection; and
5. Associating with extremist groups. ■

## 21 Observable Indicators of Possible Radicalization

**A. Self-identification** - the way individuals define their own character

**1.** Naming new ideological leaders/role models
**2.** Lingering concern with questions of meaning and identity
**3.** Concentrated self-image
**4.** Very strong devotion to a particular change
**5.** Newfound patriotism

**B. Us vs. Them Societal View** - individuals see society as a whole as an opposition to which they cannot relate

**6.** Seeing society as the enemy
**7.** Verbal expression against the government
**8.** Expressed feelings of disconnection
**9.** Change in personal narrative

**C. Social Interaction** - the way individuals interact with society

**10.** Disconnecting from former community
**11.** Initiating personal violence
**12.** Forcing customs on others
**13**. Untouchable demeanor
**14**. Dependence on communication technology

**D. Persona** - individuals' personality and expression of emotion

**15.** Change in personality
**16.** Particular emotional expressions

**E. Association** - relationships with, or representation of connection to, radical groups

**17.** Associating with extremist groups
**18.** Word choice
**19.** Change in physical appearance and/or attire
**20.** Internet identity
**21.** Training travel

# NEWS BRIEFS

## Smart TVs in Corporate Settings Could Be Easy Pickings for Cybercriminals

Cybersecurity experts have recently warned that smart TVs in corporate settings are likely to become the targets of cybercriminals, as the built-in defenses on the devices are far weaker than security on smartphones and computers. The TVs are being pushed to market quickly and security on the devices are a mere "afterthought" to manufacturers, warn experts like Candid Wueest, a threat researcher with Symantec. It's only a matter of time before there are widespread attacks against smart TVs, they warn.

## Benchmark on Detecting Breaches Indicates Improvement

Data breaches are not occurring any less frequently, but at least the time it takes to detect them is declining. In 2014, at companies that experienced breaches, 50 percent said the average time to detect an impacted system was one week or less. This number jumped to 67 percent in 2015 (see the figure on page 1).

In keeping with the year-over-year decrease in average detection time, the shortest time to detect (the same day) increased to 71 percent in 2015, from 58.5 percent in 2014 (*2015 Analytics and Intelligence Survey*, SANS Institute, Nov. 2015).

## Perceptions of Workplace Safety After San Bernardino

In the wake of the San Bernardino attack, consumer research firm C4 asked the public how safe they feel in different environments. The public feels safest at home (97 percent), while 82 percent said they feel safe at stores or the mall (82 percent) and 77 percent feel safe at work and at the movies. Sixty-five percent feel safe at the airport; 59 percent at a concert; and 58 percent at sporting events.

In general, it appears the public is beginning to resolve themselves to a new normal as it relates to violence and domestic terrorism. Some 71 percent of people think shootings like the one in San Bernardino have become a permanent part of American life, according to a NBC/ *Wall St. Journal* poll in December.

## "Special Relationship" with Employees Leads to $8 Million Settlement

In addition to losing sensitive company information and suffering protracted embarrassment in the press, the data hack of Sony Pictures is costing the company as much as $8 million to settle a claim by employees over theft of their personal information. Sony will also provide identity protection services for employees who join the settlement. The claim alleged Sony had suffered multiple attacks in the past and was aware its security was inadequate but did not take measures to prevent the data loss.

A District Judge had rejected a bid by Sony Pictures Entertainment Inc. to dismiss the lawsuit in June 2015. The ruling said Sony created a "special relationship" with employees by requiring them to provide personal information to be eligible for salaries and benefits. That relationship justified the bid by employees to hold Sony liable for its "business decision" not to enhance security after the earlier breaches.

## Are Pharmacy Delivery Vans the New Brinks Truck?

Highly sought after drugs such as OxyContin are driving a surge in robberies of delivery vans that transport prescription pills from warehouses to pharmacies and hospitals. The attacks on courier vans often involve the use of weapons and typically occur near the destination, such as pharmacy parking lots.

FreightWatch International, a provider of logistics security services, says pharmaceuticals make up 98 percent of all "last mile" cargo thefts. The number of such thefts is up fourfold over the last two years.

## More Hospitals Adopt Two-Factor Authentication– But Half Don't Have It

To enhance security and comply with HIPAA requirements to protect electronic protected health information (ePHI), hospitals are increasingly using two-factor authentication, which requires users to provide at least one additional form of identification beyond user name and password to gain access to ePHI.

As of 2014, 49 percent of hospitals had the capability

for two-factor authentication, compared to just 32 percent in 2010 (*State and National Trends of Two-Factor Authentication for Non-Federal Acute Care Hospitals*, Office of the National Coordinator (ONC) for Health Information Technology, Nov. 2015).

Fewer critical access (35 percent) and small rural (40 percent) hospitals report having the two-factor authentication capability. Two-factor authentication capability is significantly higher in medium (59 percent) and large (63 percent) hospitals than other hospital types.

The study found that two-factor capability varies significantly by location. States with the highest percentage of hospitals with the capability are Ohio (93 percent) Vermont (83 percent), and Delaware (81 percent). States with the lowest percentage of hospitals with the capability are Montana (19 percent), North Dakota (23 percent), and Maine (26 percent).

"HIPAA offers two-factor authentication as a possible method to provide security to ePHI. In addition, two-factor authentication is an essential capability for providers who e-prescribe controlled substances," concluded the ONC data brief.

## Low-Wage Workers Susceptible to Workplace Violence

Low-wage workers experience unlawful harassment and violence at work at higher rates than more highly paid workers do. This is most directly related to the type of work they perform, such as providing homecare, and because of the industries they work in. For example, workers in the restaurant industry, which employs many low-wage workers, are particularly likely to experience sexual harassment and sexual violence, notes a new study ("Workplace Violence and Harassment of Low-Wage Workers," *Berkeley Journal of Employment & Labor Law*, Vol. 36, issue 1, 2015).

Restaurant Opportunities Centers United finds that women working in the restaurant industry report having faced sexual harassment at a disproportionately high rate, the study notes. Although restaurant workers make up only 7 percent of women in the workforce, restaurant workers accounted for 37 percent of the sexual harassment complaints brought by women to the EEOC.

Low-wage workers also suffer more violence and harassment because they are less likely to assert their rights, the study concluded. "Unfortunately, low-wage workers face a wide-range of overlapping barriers when seeking justice for workplace harassment. Although workers who are harassed in the workplace know the injustice of the situations they face and want to better these poor conditions for themselves and others, they may not know where to turn for help. Low-wage workers have little information about their legal rights and where to seek justice."

Such workers are also less likely to be believed, assert the study's authors. "Internal company dynamics impact the objectiveness of an internal investigation. When it is a supervisor's word against a low-wage worker's, the company is much more likely to believe the supervisor."

To address risks faced by low-wage workers, supportive employers may want to conduct awareness-raising campaigns to help victims come forward and to discourage harassment. "The more educated the workforce is, the less likely it is that a perpetrator will think that he or she can get away with workplace violence and harassment without detection." Awareness campaigns need to cross cultural barriers and be provided in many different languages, the study notes.

## Hacked Company Sues Cybersecurity Firm for 'Malpractice'

In a first-of-its-kind lawsuit that could set an important legal precedent for the forensics/investigation practice, Affinity Gaming filed a lawsuit against its former cybersecurity firm, Trustwave, which it had hired to investigate a data breach. "At the conclusion of its investigation, Trustwave represented to Affinity Gaming that the data breach was 'contained' and purported to provide recommendations for Affinity Gaming to implement that would help fend off future data attacks," according to the complaint.

Soon after, however, Affinity discovered they'd again been hacked. "Trustwave had failed to identify the entire extent of the breach," reads the complaint. "In reality, Trustwave lied when it claimed that its so-called investigation would diagnose and help remedy the data breach, when it represented that the data breach was 'contained,' and when it claimed that the recommendations it was offering would address the data breach."

Trustwave disputes the allegations and announced that it will "defend ourselves vigorously in court." If Affinity wins on its claim, several legal analysts predict a flood of similar suits in the future. ■

## 5 Tips to Impress OSHA Compliance Officers

continued from page 1

by patients. The Minnesota OSHA office, for example, just issued the state's Dept. of Human Services a $63,000 fine for incidents in early in 2015 at Minnesota Security Hospital (St. Peter). Minnesota OSHA said staff injuries from assaults at the hospital jumped 24 percent in 2015. (For more on OSHA's enforcement focus, see "OSHA eyes workplace violence in healthcare," *SDR*, p. 3, Jan. 2016.)

### What does OSHA like to see?

It can be tough to know precisely what OSHA believes constitutes adequate protection given the absence of a specific OSHA workplace violence standard. The agency offers lots of guidance on creating and administering a workplace violence prevention program (see resources at www.osha.gov/dsg/hospitals/workplace_violence.html)—but what specific program elements seem to impress the agency?

Combing the agency's literature reveals 5 useful examples of program elements that OSHA suggests are model.

**1.** Address violence prevention in labor agreements. OSHA praised Providence Hospitals (104 beds; Holyoke, Mass.) for addressing violence prevention activities and definitions in a new contract with nurses following a period of rising incidents. "The joint efforts of labor and management have led to more than a decade of collaboration on preventing workplace violence, a multidisciplinary task force, an open dialogue, a greater emphasis on prevention and de-escalation instead of restraint, and ultimately a decrease in the number and severity of assaults by patients." OSHA loves to see the inclusion of all stakeholders in violence prevention planning.

**2.** Define your terms consistently. OSHA wants large health systems to strive for consistency in reporting and data analysis, and standard definitions make that possible. For example, the agency applauds Ascension Health—the nation's largest Catholic and not-for-profit health system with more than 150,000 associates at 1,900 locations—for its "standardized definition of workplace violence across its locations." *Ascension Health's OSHA-approved definition?* "A threat or act of violent behavior, against oneself, another person, or a group that either results in or has a high likelihood of resulting in injury, death, or psychological harm. These events may involve patients or family members, visitors, volunteers, vendors, physicians, or other associates. Examples include bullying, hostility, intimidation, or use of physical force, weapons, or power."

**3.** Increase accessibility to trainers. Periodic staff training in de-escalation techniques is a minimum requirement to steer clear of an OSHA citation, but the agency recently promoted a program at Sheppard-Pratt Health System as a good way to push knowledge to staff when they need it. "This large behavioral health system has a team of trained trainers embedded in units throughout its facilities," notes OSHA. "[They are] available to coach and mentor their colleagues in real time. For example, a trainer might step in to help a colleague who is having difficulty with de-escalating a patient. Real-time, in-unit training offers the benefit of realistic demonstration, an immediate opportunity to apply a skill, and the relevance that comes with learning in one's actual work environment."

OSHA also applauded the "train the trainer" approach used at Saint Agnes Hospital (Baltimore, Md.), where instruction is delivered by a diverse group of staff who have been certified as trainers. They include bedside nurses, team leaders, nursing supervisors, human resources staff, critical care personnel, medical/surgical staff, and security workers—"with the aim of providing mentors, coaches, and "champions" throughout the hospital."

**4.** Use technology to target elevated areas of risk. OSHA's primary focus is on programs but it promotes security technology when it's targeted at reducing the risk of violence to staff, like the use of technology at St. Vincent's Medical Center (SVMC). "[Its] director of safety and security has implemented a multi-pronged strategy to minimize risk, especially from forensic patients from nearby correctional institutions, including:

- Protocols for information exchange before patient arrival.
- A locked vestibule system where incoming forensic patients disrobe and change into hospital attire while being observed by trained staff through a one-way mirror.
- Electronic staff identification badges with a card that can be removed to trigger an alert to the security office. These badges carry GPS locators so that security staff can respond to the exact location of the alarm without delay."

OSHA also highlights engineering security controls in use at Saint Agnes and Providence Behavioral Health Hospital, which include security cameras, panic buttons, enclosed and locked emergency department reception areas, swipe card systems on key entryways, and metal detectors at high-risk clinics. It also applauded their environmental controls, such as soothing wall colors, noise reduction materials and limiting overhead pages, and establishment of quiet areas.

**5.** Assess risk from patients. OSHA stresses the importance of procedures for tracking and communicating information regarding patient behavior and special procedures for patients with a history of violent behavior. The agency praises St. John Medical Center (Westlake, Ohio), for example, for its frequent patient assessments. "Staff assess patients on admission and every two hours thereafter using a risk assessment tool. For patients deemed to pose a risk of violence, St. John developed a "code orange" system in which orange magnets are placed on door frames as a warning. Upon seeing an orange magnet, nurses look up a patient's history and enter the room with a team or a security officer, depending on the patient's care plan." The agency also praised another hospital's idea to have all patients at risk of violence wear gray gowns so staff can quickly identify them and take extra precautions. ■

# Do You Need a Drone Policy? What Should it Say?

We've previously identified emerging security applications for unmanned aerial aircraft, as well as the risks they carry. Those risks should compel organizations and their security teams to develop a policy prohibiting or governing their use, according to Sarah Moore, a partner in employment law firm Fisher & Phillips.

Activists have used unmanned aerial vehicles (UAV) to spy on pig farms, prisoners have used them to smuggle drugs, hobbyists have used them to create havoc at the White House and tennis' U.S. Open—and that was all before an estimated 400,000 people found the devices under their Christmas tree in 2015. More UAVs in more hands multiplies the prospect of adversaries using them to conduct aerial surveillance and of employees or other stakeholders using them carelessly, creating potential risks for companies to privacy, safety, and trade secrets.

"It's critical to take control of the airspace within and above your buildings, including parking lots and green spaces. You should start by crafting a policy that identifies 'no drone zones' both inside and outside," Moore told *Forbes* ("Does Your Business Need a Drone Policy?" Dec. 29, 2015). *Some considerations:*

**Response.** If an organization decides to develop a policy prohibiting the use of UAV on or above its property, then response procedures for security staff should accompany it. How is staff to respond to a drone in its no-fly area? Will the event be reported to law enforcement or the FAA?

**Notification.** If an organization uses UAV for security purposes then company policies might want to include a notice to workers of that surveillance. Although federal law does not mandate such notification, state/local laws may, and so may labor agreements, which probably makes notification the smart thing to do.

**Prohibition.** Moore thinks the average company should explicitly prohibit employees and other stakeholders from bringing UAV to the workplace to avoid "potential legal exposures."

**Permission.** There are environments in which UAV are useful and perhaps even critical to fulfill the organization's mission, such as universities or other research facilities. There may also be occasions when they simply come in handy, such as a contractor using one to efficiently conduct roof inspections. In cases where a flat "no fly" rule is not desired, then an organization's policy should identify the conditions that must be met before stakeholders operate one (see the accompanying sidebar for sample policy wording regarding permissions that a campus or organization might want to adapt).

**Privacy.** In cases where use of UAVs is allowed for purposes of recording or transmitting visual images, a company's policy should warn operators to take all reasonable measures to avoid intrusions into areas normally considered private.

**Safety/Restrictions.** Operators who receive a permit to operate a UAV on an organization's property should be warned of the safety risks and given notice of "off-limit" areas.

**Enforcement.** A UAV policy should include a statement on how violations of the policy will be handled. ■

## Sample UAV Policy—Permissions Section

The operation of a drone or UAV (unmanned aerial vehicle) over [Company] property is prohibited in the absence of approval by the [Company Chief Security Officer].
In order to obtain permit approval for the operation of a drone or UAV over [Company] property, the operator must file an application with the Security Office at least 72 hours prior to the planned operation. Application forms may be obtained at the [Security Office]. The operator must include on the form the following information:

- Exact date, time, and location of the operation;
- Purpose of the operation;
- Equipment to be used;
- Identity and contact information of the individual operating the UAV;
- Data to be collected; and
- Evidence of Federal Aviation Administration approval of UAV operation (such as a current 333 exemption or Certificate of Waiver or Authorization (COA) issued by the FAA or documentation verifying that the individual operating the UAV is fully authorized by the FAA to do so).

The proposed operation must not pose an unacceptable threat to safety, privacy, or the environment. Approval, once given, may be rescinded if it is determined that the information provided is incorrect or incomplete or if circumstances have changed and a determination is made that the planned operation is not in [Company's] best interest. [Company] also reserves the right to immediately order the cessation of any operation that is deemed to create a hazard or interference with any [Company] equipment or activity.

## Is Your Company's Hotline Serving Security's Goals?

continued from page 1

surveys by service providers. *For example:* 37 percent of companies experienced an increase in calls in 2012-2014 compared to the previous two-year period. Only 12 percent saw a decline during the same period (*Helpline Calls and Incident Reports*, Society of Corporate Compliance and Ethics (SCCE), 2014).

But while the number of calls has increased, employers haven't suffered a spike in whistleblower lawsuits, according to the SCCE. "It appears, at least to date, that employees are trusting their employers to respond to issues when they are formally reported," the report concluded. "It will now be critical for organizations to respond effectively and expeditiously to the increased employee reports of wrongdoing. If responses languish, if allegations are not reviewed, if those making allegations are not communicated with effectively, employees may quickly lose faith in their employer and turn to outsiders, including attorneys and the government, when they see wrongdoing."

The value of a company compliance/ethics hotline as a theft prevention and investigative tool is not assured. Operational and technical issues–or simple neglect–can limit the effectiveness of hotlines.

**Benchmarks.** Companies with fewer than 5,000 employees typically have the highest incident report rates, 15.72 reports per 1,000 employees, according to The Network, Inc., a hotline provider (*2014 Corporate Governance and Compliance Hotline Benchmarking Report*). Companies with 20,000 to 50,000 employees were next, with 9.43 incident reports per 1,000 employees.

**As an investigative tool.** The value of a company compliance/ethics hotline as a theft prevention and investigative tool is not assured. Operational and technical issues—or simple neglect—can limit the effectiveness of hotlines. For example, after abuses were uncovered at a poultry supplier to Purdue Farms, *USA Today* said it confirmed that the phone number in employee manuals for a Perdue hotline went straight to a fax machine.

Company hotlines serve many stakeholders, including human resources, finance, environment, health, and safety. Indeed, hotline provider NAVEX Global says that more than half of the incident reports it logs are personnel related—wages, hours, benefits, diversity, or workplace respect issues (*NAVEX 2014 Ethics and Compliance Hotline Benchmark Report*). Additionally, the primary function of hotlines operated by or for public companies is to satisfy compliance with requirements under Sarbanes-Oxley to facilitate confidential and anonymous reporting of misconduct, fraud, or other concerns. For these companies, helping the security department combat fraud is far less important.

### Get security value from your company's hotline

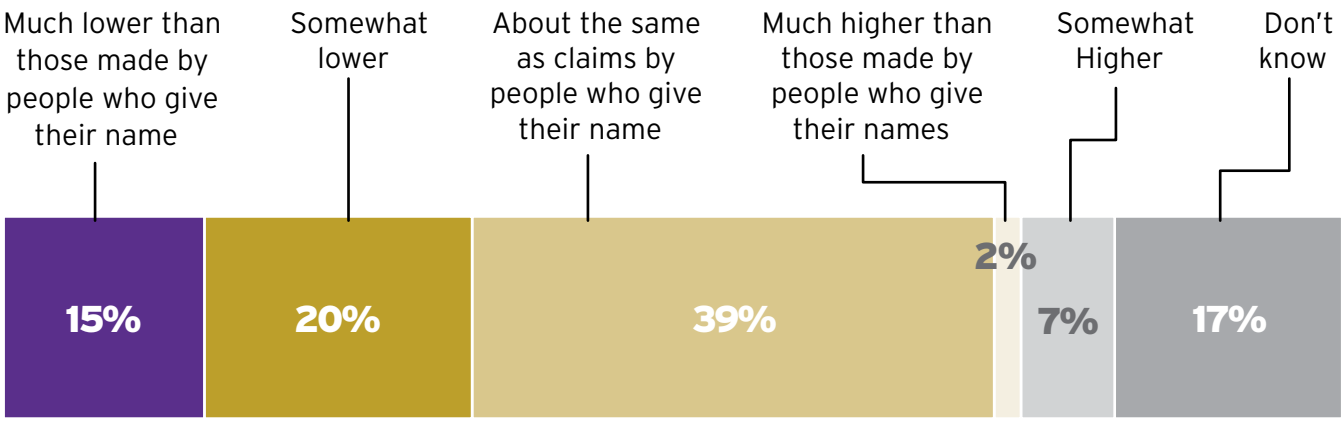
Security directors, consultants, and hotline providers suggested some questions worth asking.

**Is it being promoted?** The number of security tips that a hotline receives directly correlates with how familiar employees are with the program. In addition to a traditional integrated communications campaign (wallet cards, paycheck stuffers, new employee orientation, emails, posters, newsletter, code of conduct), security directors should extend program awareness to include the employees of suppliers and contractors. Employees of a supplier are often willing to alert a client to fraud by his/her company and listing the hotline number on checks issued to suppliers is an inexpensive action that has helped uncover fraud for many companies, according to hotline providers. To maximize incident capture, hotlines should be available 365/24/7 (only half of hotline calls occur during business hours) and have intake operators who can communicate with non-English speaking employees.

**Is it being promoted as an *alternative* for security incident reporting?** People have a preference for internal, in-person reporting, according to the recent surveys. This suggests that not everyone who has information about theft, fraud, or other security issues will want to use a hotline—especially one run by an outside company—to report it. A hotline provides an alternative way for employees to report security problems, but it should not be presented as a substitute for reporting security concerns to the security department or through other internal channels (i.e., security departments need to maintain an open-door policy).

Some companies find it best to promote an ethics hotline to handle complaints and concerns on accounting matters but to direct employees to report concerns relating to security issues to their supervisor, HR, or the security department. Others maintain a unique security hotline managed by internal security staff in addition to an ethics hotline. In all cases, however, intake operators should be directed to accept calls of all types, as it's unwise to

## The Substantiation Rate of Claims Made Anonymously Is...




*survey of 677 compliance professionals

(Source: Society of Corporate Compliance and Ethics, 2014)

People have a preference for internal, in-person reporting, according to the recent surveys. This suggests that not everyone who has information about theft, fraud, or other security issues will want to use a hotline—especially one run by an outside company—to report it.

tell a caller to hang up and call a different number.

**Are you getting the reports you need?** A hotline program needs a clear set of rules for how, when, and to whom information from tips is disseminated. Since many types of calls are received by hotlines, security directors should be sure that the protocols are such that the security department is receiving notice of all reports that it wants to receive.

**Are operators sufficiently trained?** To discourage bogus calls, operators should be able to conduct probing, in-depth telephone interviews so they can distinguish legitimate information from that which seems solely designed to intentionally damage an individual's career.

For this reason, hotline reporting via live operators is preferable to anonymous email, website complaints, or answering machines. These can be used to supplement the main hotline, but online methods don't permit interviewers to ask follow-up questions or seek clarification, and so are more likely to be used by individuals making false reports, which can result in countless wasted hours by investigators. Finally, person-to-person reporting systems allow interviewers to provide anonymous callers with a unique identifier to facilitate the making of follow-up reports, while electronic submissions don't encourage an on-going dialogue with a tipster.

The importance of the individuals who handle tips is reflected by the belief of many that anonymous reports are not as reliable as non-anonymous reports (see the accompanying figure).

**Are emergency protocols clearly identified?** A call to a hotline to report minor theft and a call that suggests an imminent threat of violence demand different responses. Call centers (or internal call operators) must have clear direction for the types of incidents that demand immediate, expedited reporting (workplace violence, release of proprietary information, etc.) versus incidents that can be processed via the normal dissemination process (i.e., bogus expense account charges).

**Are you periodically testing the hotline for performance?** To ensure hotlines are serving your security goals, periodically test intake operators' interview style, questions, and performance, as well as the quality and timeliness of the subsequent report to the security department. ■

### Coming in future issues of SDR

- Is Your Strategic Plan at Risk of Being Derailed? Identify Events That Could Doom Your Operation
- Secrets to a Successful Massive Security Technology Roll Out
- What Is Your Security Firm Doing to Track Performance? Here's What They Should Be Doing
- Buried Under a Pile of Data? How to Use Data to Your Advantage Instead
- Is Your Video Surveillance System Providing Maximum Benefit? (Probably Not)
- Better Predictions, Better Security—Learn How Some Security Leaders Can See the Future

**PERIODICALS**

SECURITY DIRECTOR'S REPORT
P.O. Box 92558
Long Beach, Ca 90809

## JOIN TODAY!

◯ **YES!** I'd like to receive the next 12 issues of the SECURITY DIRECTOR'S REPORT for $295, a $100 savings off the regular subscription price.
Discount code SDRMAR.

◯ **YES!** Rush me SECURITY POLICIES, PRACTICES AND MANAGEMENT STANDARDS for only $345

☐ Enclosed is my check for $_____.

☐ Bill me/my company.

☐ Charge my: ____Visa ____MasterCard ____AMEX

Card # Exp.

Telephone - Home Office

Name

Title

Company

Street

Email

City State ZIP

**Security Director's Report**
P.O. Box 92558
Long Beach, Ca 90809

*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.

**Phone: 888-881-5861 or fax to: 714-226-9733**

# Security Policies, Practices and Management Standards

### Technology-Driven Security Comes Up Short

Technology is central to today's security efforts, but a company's security policies, practices and strategies are the true source of comprehensive, successful protection and loss prevention. Security Policies, Practices and Management Standards report helps you fine tune your strategy and operations with extensive research on the policies, procedures and best practices utilized by over 300 organizations.

### We've Done the Work So You Don't Have To

Based on exclusive data from national surveys, you'll find out the policies and procedures organizations use most frequently to structure and implement cost-effective programs that meet today's evolving threats and manage crisis, all in one report. Compare your initiative with industry practices in:

- Violence prevention policies, strategies and tactics
- Building access management and fraud prevention
- Effective, compliant employee monitoring and surveillance practices

This report is not advertiser supported so you can count on unbiased findings on how companies structure operation control and responsibilities, integrate physical and network security, the frequency of threat assessments, and the practices security executives believe are most important to securing company information. These findings and much more will help you shape and update your strategy to improve protection and reduce costs.

**No Risk Offer:** Order your copy today on the coupon to the left or call 888-881-5861 and ask for report 3971. You pay just $345 (plus $16.95 shipping/handling). If you are dissatisfied with your report for any reason, return it within 30 days and you'll receive a full refund—that's 100% Money-Back Guarantee, with no questions asked.