ASIS Banking & Financial Services Council Newsletter

VOLUME 11, EDITION 3 JULY—SEPTEMBER 2017

ASIS News

New ASIS Standards Initiative to Address Active Assailants

Today, ASIS International announced it will develop an *Active Assailant Supplement* to its existing *ANSI/ASIS/SHRM Workplace Violence Prevention and Intervention Standard (WPVI).* With the addition of this supplement, security professionals will have an enhanced standard for practical methods to develop an effective approach to prevention, intervention, and response to an active assailant—either acting alone or in a group.

"Workplace violence is one of the most significant security and personnel safety challenges facing organizations today," said Gene Ferraro, CPP, PCI, SPHR, SHRM-SCP, chair of the standard technical committee and chief executive, Forensic Pathways, Inc. "Of the many facets of workplace violence, active assailant is the most concerning, because it is the deadliest. Globally, in both the public and private sector, security professionals are searching for solutions. This standard will provide much needed direction and guidance."

The supplement will include security design considerations, protocols, and response strategies, as well as procedures for detection, assessing vulnerabilities, and managing and neutralizing immediately life-threatening behavior perpetrated by an active assailant. While the original WPVI standard focused on prevention and intervention, the supplement addresses onsite response specific to an active assailant or shooter event.

"As the leading association for security management professionals globally, ASIS International has the expertise and practical experience within its membership ranks to lead this effort," said Michael Crane, CPP, co-chair of the technical committee. "By tapping into this expertise from across the public and private sector—as well as reaching out to key stakeholders across the security spectrum—we will deliver a standard that provides actionable information and guidance to effectively address these low probability, but high consequence, situations. Ultimately, proper preparation and planning will diminish casualties and save lives."

ASIS INTERNATIONAL
Advancing Security Worldwide®

Upcoming Programs and Webinars

11 October 2017

Active Shooter in High Rise Environment: Critical Differences

15-20 October 2017

ASIS/Wharton Program for Security Executives

25 October 2017

The Cost Impact of GDPR and Privacy Regulations for Physical Security

25 October 2017

Food Defense: From Theory to Reality

5 -7 November 2017

ASIS Middle East 2017

6 -7 November 2017

Security Force Management

6 - 8– November 2017

Conducting Advanced Internal Investigations

6 -8 November 2017

Risk, Threat, and Vulnerability Assessment

8 November 2017

Advantages of Wireless for Commercial Security

9 –10 November 2017

Executive Protection

9 –10 November 2017

Soft Target Hardening

IN THIS ISSUE:

In The News

Why Europe Has a Greater Terror Problem Than the United States
USA Today

According to the University of Maryland's Global Terrorism Database, there were 100 attacks that killed 97 people in the U.S. in 2015-2016, compared to 604 attacks that claimed 383 victims in Western Europe during the same time period. "There are oceans separating North America from the main conflict zones in the Middle East and Africa," where recent terrorists have been radicalized, said Phil Gurski, a former Canadian intelligence analyst who runs a risk consulting firm. "It is far easier for extremists to get to Italy from Libya than it is for them to go from Libya to Canada or the U.S." PeaceTech Lab, a group that analyzes conflict-related data, noted that so far this year, at least 39 people have been killed in 11 terrorist attacks in Western Europe, compared to five attacks in the U.S. that have caused seven fatalities.

Nearly 30 Percent of Travel Managers Are Unsure About Locating Employees in Crisis Situations
Meetings & Conventions

According to a new study released by the Global Business Travel Association (GBTA), 29 percent of travel managers say they do not know how long it would take to locate their affected employees in a crisis situation. The report also found that 50 percent of travel managers say that in the event of an emergency, they can locate all of their employees in the affected area within two hours or less. In addition, 60 percent of travel managers rely on travelers to reach out if they need help and have not booked through proper channels. "Failing to establish and communicate safety measures leaves travelers and organizations vulnerable," said Kate Vasiloff, the GBTA Foundation's director of research. "As both security threats and technology evolve, even the most robust protocols that once served companies well may now have weaknesses requiring immediate attention and modification." Once it has been determined travelers are in an area experiencing a security threat, every minute spent trying to get in touch could be putting them in greater risk. Live personal calls (58 percent) and automated emails to business addresses (52 percent) are the most popular methods of communicating with travelers in a crisis. To manage the complexity that comes with building and maintaining a robust duty-of-care program, 65 percent of organizations retain the services of third-party safety and security firms.

Psychological Price
Security Management Organizational counterterrorism planning can benefit from understanding the psychological impact of terrorism. Psychological concepts can help security practitioners mature and validate their plans. Security professionals must understand the different types of behavioral reactions associated with emergencies ranging from anthrax scares to armed intruders to properly plan for different types of events. PTSD is a possible psychological consequence of any traumatic event, but the likelihood of this condition varies. Active shooter and other purposefully violent events result in mental health diagnoses at a level almost three times higher than the diagnoses after natural disasters. Distinguishing conventional from unconventional terrorism will help emergency management experts plan for various types of events. Conventional terrorism is the use of shooting, bombing, kidnapping, and hostage-taking. Unconventional terrorism involves more exotic weapons, such as chemical, biological, radiological, and nuclear materials. The timeline of an attack, and the amount of time that has passed since the incident took place, also play a crucial role in shaping the response. Training in psychological first aid helps for better response to a violent or traumatic events.

In The News

FBI Says ISIS Used eBay to Send Terror Cash to U.S.
Wall Street Journal

A senior Islamic State official funneled money to an alleged ISIS operative in the U.S. through fake eBay transactions, according to a recently unsealed FBI affidavit. The alleged recipient of the funds, an American citizen in his early 30s, was part of a global network stretching from Britain to Bangladesh that used similar schemes to fund Islamic State and was directed by a now-dead senior ISIS figure in Syria, Siful Sujan. Mohamed Elshinawy had been arrested more than a year ago in Maryland after a lengthy Federal Bureau of Investigation surveillance operation that found the first clues to the suspected network. The government had alleged in a 2016 indictment that he pledged allegiance to Islamic State and had pretended to sell computer printers on eBay as a cover to receive payments through PayPal, potentially to fund terror attacks. The case suggests how Islamic State is trying to exploit holes in the vast online financial world to finance terror outside its borders.

Twenty Percent of U.S. Workers Find Workplace Hostile or Threatening
Chicago Tribune

The American workplace is grueling, stressful, and surprisingly hostile, concludes a new, in-depth study of more than 3,000 U.S. workers by the Rand Corp., Harvard Medical School, and UCLA. The research found that nearly one in five workers say they face a hostile or threatening environment at work, which can include everything from bullying to sexual harassment. Nearly 55 percent of respondents say they face "unpleasant and potentially hazardous" conditions, while almost 75 percent say they spend at least one-quarter of their time on the job in "intense or repetitive physical" labor. Only 38 percent say their jobs offer good prospects for advancement, and 50 percent say they work on their own time to meet the demands of their job.

Bombing Plot in Oklahoma City Is Thwarted With Arrest, FBI Says
New York Times

Federal officials report a 23-year-old Oklahoma man has been arrested after he tried to blow up a bank in Oklahoma City using a vehicle bomb similar to the one that destroyed the federal building there in 1995. The man, Jerry Drake Varnell, had been plotting the attack for months, the authorities said, but was thwarted by a long-running undercover investigation led by an FBI joint terrorism task force. Varnell was arrested Saturday after he parked a van loaded with what he believed to be a working explosive device in an alley next to the bank.

Mitigating Active Shooter Risks
PropertyCasualty360

Security professionals should prepare their companies for the possibility of an active shooting, as the number of incidents involving active shooters has risen steadily over the last 15 years. Keith Plaisance of Global SHE Solutions says implementing an active shooter program is similar to preparing for a fire drill, and survival depends on having a plan with three specific options: run, hide or, fight. Preparing for an active shooter scenario involves the development of a workplace violence policy and plan, emergency response plans, training, and exercises. For the workplace violence policy, the employer should establish acceptable workplace behavior, affirm the company's commitment to take action and provide a safe workplace for employees, and address physical violence as well as threats, bullying, harassment, and weapon possession. Plaisance says a reporting mechanism should be in place letting employees know who to approach with concerns. He also recommends creating a threat assessment team within the company. Companies should test plans to determine effectiveness and identify potential problems, presenting plans to employees in regular training. Companies should also conduct a detailed physical security assessment, with the goal of denying unauthorized access and protecting property, personnel, and operations.

Cyber Security

U.S. Senator on Equifax Hack: 'Somebody Needs to Go to Jail'
New York Times

Thirty-six U.S. senators on Tuesday called on federal authorities to investigate the sale of nearly $2 million in shares of credit bureau Equifax Inc by company executives between July 29 - the day Equifax said it learned that its systems were hacked in mid-May - and when they made it public last week. "If that happened, somebody needs to go to jail," said Senator Heidi Heitkamp, a Democrat on the Senate Banking Committee. Cybersecurity experts believe the breach is one of the largest data hacks ever disclosed. Equifax Chief Executive Officer Richard Smith apologized for the breach and vowed the company "will make changes," but did not address the stock sale issue. In their letter, the lawmakers, led by Jack Reed, a Democrat, and John Kennedy, a Republican, requested "a thorough examination of any unusual trading, including any atypical options trading, for violations of insider trading law."

Equifax Breach Prompts Scrutiny, but New Rules May Not Follow
New York Times

U.S. authorities and consumers are calling for more oversight of credit reporting bureaus following the disclosure of a major data breach involving Equifax that has potentially compromised the sensitive personal data of more than 143 million Americans. However, the push is unlikely to translate into new rules or legal curbs. The credit bureaus have for decades successfully fended off calls in Congress for more oversight, despite warnings about potential problems that go back to Senator William Proxmire, a Wisconsin Democrat, in the 1960s. Now, the industry is likely to find support in the agenda of President Donald Trump, who has pledged to strip away “burdensome” business regulations. A vocal critic of the secrecy of credit bureaus, Proxmire thought that without strict oversight, the industry might be tempted to cut corners on data protection. “Since credit bureaus are almost entirely responsive to the needs of business and have little responsibility to consumers, it is difficult to see major expenditures on security systems in the absence of public standards,” he said during congressional testimony in 1969. Proxmire helped lay the groundwork for the Fair Credit Reporting Act, but it placed enforcement in the hands of the Federal Trade Commission, which has limited supervisory powers and little ability to levy significant penalties. Forty-eight states have passed security breach notification laws, but calls for a nationwide standard have repeatedly fizzled. Equifax has recently lobbied on a range of cybersecurity issues, including “data security and breach notification,” “data breach response and identity protection” and “cybersecurity threat information sharing.”

Data Breaches Are Up 29 Percent Over Last Year
San Diego Union Tribune

There are 29 percent more data breaches occurring this year compared to last year, according to a new report from the Identity Theft Resource Center (ITRC) and CyberScout. In addition, hacking is the leading cause of data breaches nationwide, with more than 790 so far this year, exposing more than 12 million records, according to the report. The ITRC tracks breaches in the categories of financial, healthcare and medical, government and military, education, and business. The center found more than 50 percent of all breaches this year have occurred in business, followed by healthcare and medical. For this report, a data breach is defined as having occurred when a name is released in connection with a Social Security number, a driver's licensing number, or a medical or financial record. The exposure is tracked when it occurs because of a phishing or hacking attack, theft, negligence, or error. Exposure that includes a user name or email address in combination with a password or security information that would allow access to an online account could trigger notification in California, the first state to enact a data security breach notification law. So far in 2017, personal information has been compromised by the unauthorized acquisition of data at universities, business, banks, medical, and government organizations.

Facial Recognition

Editor's Note: The following article was submitted by our esteemed colleague P.K. Smith, CPP.

We often get inquiries about new technologies, and the recent buzz about video facial recognition software is no exception. Originally designed to help identify known criminals, businesses are now using the software to help identify (and market to) known customers. According to a recent USA Today article, the facial recognition market is worth approximately $3 billion, and it is expected to grow to $6 billion by 2021. Surveillance is a large reason for the growth and government entities are the primary consumers. The FBI has a database with images of approximately half of the U.S. population. Since facial recognition may soon become a popular tool in the bank security world, all bank employees should be aware of how this rapidly evolving technology works.

Facial recognition is one of several types of "biometric" identification systems, much like fingerprints or retina scans. This software based system examines the physical features of a person's body in an attempt to uniquely distinguish one person from all others. Much like a fingerprint record, this "faceprint" is a set of measurements and characteristics that, when taken together, uniquely identify one person's particular face. A faceprint may be compared with a single photo to verify the identity of a known person, like an employee trying to enter a restricted area. Faceprints can also be compared to databases of many images in the hopes of identifying an unknown person.

From a banking perspective, one can see the benefits of identifying known customers or known criminals. Think of the advantages. Wouldn't it be nice to be certain that the customer standing in front of a teller is indeed who they claim to be? No more relying on a teller's ability to verify a signature, which changes ever so slightly each time a person signs their name. Or how about the ability to show a red flag on the new account screen whenever a known con-artist is seated at the new account officer's desk? The benefits are quite clear, but like so many other facial recognition applications, the technology still has problems.

A key factor affecting how well facial recognition works is lighting. An evenly lit face seen directly from the front, with no shadows and nothing blocking the camera view, is the best. In addition, whether an image of a face contrasts well with its background, and how far away it is from the camera will have a significant impact on image quality. Another very important challenge is the degree to which the target individual cooperates with (or is even aware of) the process. When a facial recognition system incorrectly identifies a person, it can cause a number of problems. A system restricting access to a specific location could wrongly admit an unauthorized person, or it could block the admission of an authorized person thereby impeding the workflow of a critical operation. Regardless of how accurate it appears to be on television crime shows, there is room for error, though the technology is improving. The National Institute of Standards and Technology (NIST) estimates that stated error rates are declining 50 percent every two years and are currently around 0.8 percent.

It is clear that facial recognition has significant benefits in law enforcement and potential benefits to the private sector. On the other hand, those of us in the banking industry must be aware of its limitations and potential negative impacts..