ASIS Banking & Financial Services Council Newsletter

VOLUME 8, EDITION 1 JANUARY-MARCH 2014

ASIS News

We're always looking for referrals…

Please share your membership experience and the value you've received with your peers and invite them to join ASIS too. By doing so, you strengthen our global community and become eligible to win prizes.

Colin Powell to keynote ASIS 2014

General Colin L. Powell, USA (Ret.) will share leadership insights gained over the course of 50 years in public service, when he delivers the keynote address at the ASIS International 60th Annual Seminar and Exhibits, Tuesday, Sept. 30 at the Georgia World Congress Center, in Atlanta, Ga. The keynote session is open to all registered attendees.

Registration and housing for ASIS 2014 are now open.

Share your chapter's P3 success story

Applications for the 2014 ASIS Law Enforcement Liaison Council (LELC) and the Foundation's Matthew Simeone Award for Public Private Partnership Excellence are now being accepted. ASIS chapters are encouraged to share their successful programs developed in collaboration with local law enforcement agencies. The award will be presented in Atlanta at ASIS 2014. Visit www.asisfoundation.org for award details and application.

Earn your bachelor or master's degree on scholarship

The ASIS Foundation is currently accepting application for six full-tuition scholarships to University of Phoenix. All security professionals are eligible to apply through April 15. Winning professionals may earn their degree of choice from any programs offered at University of Phoenix. Classroom and online courses are available.

Applications for two full-tuition scholarships to attend Webster University will be accepted beginning March 4. Winning ASIS members will have the opportunity to complete a graduate degree in Business and Organizational Security Management. Recipients may choose to attend a Webster University on-ground campus, Webster University online, or a combination of the two.

Go to www.asisfoundation.org to learn more and apply for these scholarships.

Upcoming Webinars

April 16 , 2014
Managing Contractors Onsite

May 21 , 2014
Case Study of a Transnational Threat: Lashkar-e-Taiba

May 28 , 2014 Reducing Crime Through Community Engagement

June 4 , 2014 Critical Infrastructure Protection: The Way Ahead

June 11 , 2014
Protect Your Perimeter: Technology Solutions for Organizational Success

July 16 , 2014 Twelve Symptoms of a School with Problems

August 6 , 2014
SAFETY Act: Legal Liability Protection for Providers on Users of Effective Anti-Terrorism Products and Services

August 20 , 2014 Critical Infrastructure Protection From a Private Security Perspective

December 10 , 2014 Use of Social Media for Screening Employee Candidates & Monitoring Current Employees

IN THIS ISSUE:

In The News

Retail Security a Hot Topic as the National Retail Federation's Big Show Convenes
Brandchannel.com (01/13/14)

Retail security is expected to be a hot topic at the National Retail Federation's (NRF) 2014 BIG Show in New York City following the recent attacks on Neiman Marcus and Target. The NRF recently backed the adoption of higher security "Chip-and-PIN" cards, which the payments industry plans to fully introduce in the U.S. by 2020. Some say that these cards could have prevented the breaches at Target and other retailers. The so-called "Holiday Hack Attack 13" on Target resulted in the exposure of the personal credit information of more than 100 million customers, as well as their names, mailing and e-mail addresses, and telephone numbers. Neiman Marcus revealed Jan. 10 that it suffered a security breach that might have compromised its customers' credit cards, nothing that its credit card processor informed it in mid-December about "potentially unauthorized payment card activity" on cards that had been used at its stores. There has been some speculation that the hacks were conducted by the same group, given the timing of the attacks and the existing retail partnership between Neiman Marcus and Target, though neither retailer has confirmed that there is a connection between the attacks. Reuters has reported that there have been at least three other major U.S. retailers who faced similar attacks, and experts say there will likely be more retailers who suffer such breaches until more is done to secure consumers' personal financial information.

In a Cyber Breach, Who Pays, Banks or Retailers?
Wall Street Journal (01/12/14)

Target's recent customer data breach has many cybersecurity experts asking how it could have been prevented, and many banks and retailers wondering "Who is going to pay?" While Target is already offering free credit monitoring and identity theft protection to compromised customers, some banks have argued that retailers should pay to reissue affected credit or debit cards. Retailers, on the other hand, say that banks should take steps to protect payment cards so they cannot be compromised. Lawmakers are expected to weigh in on the debate in coming weeks, with hearings scheduled on data-security before the Senate Banking Committee. Camden Fine, the president of the Independent Community Bankers of America, says the Target incident could motivate Congress to take action on efforts to resolve the issue of who is financially responsible for data breaches.

Training Security Officers for Better Access Management
Security Magazine (01/14/14)

Enterprise security leaders should provide their security officers with training on how to effectively manage access to their buildings, since doing so can help officers better identify potential security threats. Such training should focus on a number of key points, including monitoring individuals who are attempting to access the building as soon as possible and from as far away as possible and continuing to monitor the person until he has reached his intended access point. Monitoring should focus on identifying signs in the person's appearance or body language, such as the presence of bulky items inside pockets or nervous behavior, that could be indicative of a potential threat. However, security officers should be reminded during their training that appearance and body language need to be evaluated in the context of the individual's environment before they make a determination that a person is indeed suspicious.

In The News

ASIS Releases Revised CSO Standard
Security InfoWatch (01/22/14)

ASIS has released a revised ANSI/ASIS standard governing the role of chief security officers (CSOs) within organizations to replace the 2008 ANSI/ASIS Chief Security Officer Organizational ANSI standard. The new standard will create a model that can be used by organizations developing a senior leadership function that will be responsible for providing strategies used to protect organizations from security threats. Jerry Brennan, the technical committee chairman and CEO of Security Management Resources, says the new standard will help organizations determine their needs for the senior security executive position as well as the competencies that are best suited for that position.

New ASIS PCB President: Blurring Lines Between Public, Private Sectors
Security Director News (01/31/14) Canfield, Amy

ASIS Professional Certification Board (PCB) President Owen J. Monaghan says that one of his goals for his current term, which will run through the end of the year, is to increase the number of security professionals who are ASIS-certified. Monaghan, who is also the assistant police chief of the New York City Police Department and is the first active-duty police officer to serve as president of the PCB, says one reason why he wants to promote ASIS certification is because he has benefited from having a Certified Protection Professional (CPP) designation himself. Monaghan says that having this designation gives the private private sector partners he works with in securing infrastructure, events, and venues the assurance that he is knowledgeable about security issues. Certification can benefit other security professionals as well, Monaghan says, because PCB's certs are kept up-to-date with changing skill sets and because they are relevant for any industry. In addition, security professionals who are certified have demonstrated that they have a "passion for knowledge" that is valuable in the workforce today, Monaghan says.

Are Evacuation Practices Flawed?
Security Management (02/14) Gates, Megan

Companies and institutions of higher learning have a growing number of technological solutions at their disposal to communicate with employees, students, and others in the event of active shooter situations and other emergencies. One such solution is Amerilert, a cloud-based system that allows corporate administrators to create and save custom alerts about emergency response plans before an emergency takes place. In the event of an emergency, these alerts are sent out to employees and others via various communications channels to advise them of the situation and urge them to take the proper precautions. Employees can respond to these alerts to let administrators know that they are safe and unharmed. Such systems can be used to eliminate the practice of having employees assemble at rallying points following an evacuation, which is currently seen as a best security practice even though it could potentially open up he possibility of workers being injured or killed in follow-up attacks, said Nater Associates President Felix Nater.

5 Steps for Successful Lockdown Procedures
Security Magazine (02/14) Dalton-Noblitt, April

Every organization should have a lockdown strategy that governs the state of every opening of the building both on demand and during an emergency situation. Defined by two aspects - security zones and people and processes - lockdown strategies must be clearly established and practiced. There are several steps that organizations can take to ensure that their lockdown strategy provides their building or facility with the greatest amount of protection. The strategy needs to be designed for each layer of security from individual rooms to the perimeter of the facility's campus, with adjustments being made to ensure clear line-of-sight surveillance and entranceway monitoring. Additionally, organizations need to determine what type of lockdown solution or solution combination will best suit their facility and then will need to ensure that building lockdown procedures and preparations are detailed and maintained. Organizations will also need to learn what types of hardware or methods to avoid using and will need to make sure that lockdown standards are understood. Together, these steps will help ensure that an organization's lockdown procedures are successful.

Cyber Security

Senior Managers are the Worst Information Security Offenders
Help Net Security (01/08/14)

Senior managers pose a major security risk for companies, according to a Stroz Friedberg nationwide survey of 764 information workers. The survey found that 87 percent of senior managers frequently or occasionally send work materials to a personal cloud or email account in order to work remotely, which makes such information more vulnerable to breaches. In addition, 58 percent of senior management reported having accidentally sent the wrong person sensitive information, compared to just 25 percent of workers overall. When leaving past employers, 51 percent of senior management and 37 percent of mid-level management acknowledge taking job-related emails, files, or materials with them, while just one-fifth of lower ranking employees did so. In addition, just 35 percent of respondents reported receiving regular training and communications on mobile device security from their employers, 37 percent on social media use, and 42 percent on information sharing.

Global Cyber-Attackers Diversifying their Techniques: Crowdstrike
eWeek (01/23/14)

CrowdStrike says hacktivists, nation-state-backed groups, and cybercriminals are becoming increasingly sophisticated and their attacks more numerous. The annual CrowdStrike report notes a number of trends, one being that while groups linked to China continue to account for the majority of attacks targeting intellectual property and classified information, groups from the Middle East, Russia, and Asia are also carrying out an increasing number of attacks. Such groups include the Syrian Electronic Army, which has made a name for itself by defacing the websites of many global companies and, more recently, targeting third-party service providers. However, the major trend highlighted in the report is the increasing use of strategic website compromises (SWCs), also known as watering hole attacks, where hackers compromise a legitimate site with the goal of infecting specific visitors with malware. CrowdStrike says the attacks are especially popular with Chinese groups, pointing to the attack that compromised the website of the Council on Foreign Relations in December 2012 as one of the earliest examples. CrowdStrike says hackers looking to invade and spy on enterprise networks are likely to turn to SWCs as traditional spear phishing email attacks become less effective.

Experts Warn of Coming Wave of Serious Cybercrime
Washington Post (02/10/14)

Experts say a string of recent retail data breaches could be a preview for a major wave of hacks against U.S. payments systems that antivirus software and account monitoring tools cannot deter. Experts say the rise in data breaches can be countered by technology upgrades, including the adoption of end-to-end encryption, isolating the most sensitive data on separate networks, and using newer credit card technology that stores customer information on an embedded chip. Meanwhile, security experts stress that companies should install systems that spot and block intrusions swiftly, before massive volumes of personal data can be stolen. "Companies need to be hunting on their networks constantly...looking for signs of compromise," advises Crowdstrike Services president Shawn Henry. Long-term retail cyberattack projections are debatable, with the possibility of companies successfully fortifying their defenses in the coming months to ward off attackers, or of market saturation of stolen credit data causing prices to drop and incentives to launch new attacks to decline, says Carnegie Mellon University researcher Nicolas Christin.

Study Shows Those Responsible for Security Face Mounting Pressures
CSO Online (02/11/14) Ragan, Steve

IT security professionals are increasingly feeling stress in their jobs, according to a new Trustwave survey of 833 security decision makers in the U.S. and several other countries. Sixty-five percent of U.S. respondents expected to feel more pressure in the year ahead, up from 62 percent in the 2013 survey. When asked to explain why IT security professionals are facing a growing amount of pressure at work, Trustwave's Leo Cole and Chris Pogue offer differing explanations. Cole notes that corporate boards are increasingly focusing on why data security breaches and other incidents are continuing to happen in spite of investments in cybersecurity, which in turn is putting pressure on CIOs to stand behind the security technologies that they have purchased.

Cyber Security

Cybersecurity Firm Raises Concerns About Lenders' Practices
Los Angeles Times (03/02/14) Sichelman, Lew

The cybersecurity firm Halock Security Labs reports that mortgage companies big and small allow information-sharing practices that puts personal and financial data at grave risk. In its investigation of 63 lenders, the company discovered that seven out of 10 allowed applicants to send their information over unencrypted email as attachments. Moreover, nearly the same percentage encouraged faxing sensitive data, which is somewhat less dangerous but still not as secure as encryption. Only 40 percent of the lenders studied offered a postal mail option, and just 12 percent provided a secure email portal.

Cybercrime Tracked to Middle Managers
Investor's Business Daily (03/06/14) P. A4 Tsuruoka, Doug

A significant portion of the cybercrime dogging global businesses and government organizations can be tracked back to middle managers, according to a new report from PricewaterhouseCoopers (PwC). "Many times those who are colluding [with outside hackers] are individuals inside these companies who have administrative access to the corporate computer system," says PwC's Steve Skalak. He says in this case a middle manage" is anyone with administrative oversight of corporate computers and extends beyond system administrators. Skalak says while PwC was not able to gather information on what sorts of cybercrimes middle managers were most associated with, it is likely to focus on the theft of confidential corporate or governmental information. Nice Actimize CEO Amir Orad says middle managers are also a targets of attackers simply looking to steal high-authority credentials, meaning many managers may unwittingly become parties to cybercrime. The PwC report also found that top executives were most concerned about three aspects of cybersecurity—preventing economic espionage, implementing proper cybersecurity controls, and handling the financial, legal, and reputational fallout of data breaches.

Most Businesses Unprepared for Cyberattack, Study Finds
ZDNet (03/18/14) Osborne, Charlie

Many organizations around the world are unprepared to deal with cyberattacks, even though such attacks are common, according to a new survey by the Economist Intelligence Unit and Arbor Networks. Of the 360 business leaders who participated in the survey, 38 percent said their organizations had no cyberattack response plans in place, even though 77 percent said their firms had experienced at least one security breach over the previous two years. The survey also found that only 17 percent of organizations believe that they are fully prepared to deal with a cyberattack. When respondents were asked what would help them be better prepared for cyberattacks, 41 percent said they needed a better understanding of potential cybersecurity threats against their organizations. But the survey indicated that information about such threats may be hard to come by, as only about 33 percent of organizations share data about cybersecurity attacks with others. Organizations may be hesitant to share information about cybersecurity attacks due to fears that their reputation could be harmed if they do so. Another 57 percent of respondents said they do not voluntarily report successful cyberattacks if they are not required by law to make such disclosures.

U.S. Notified 3,000 Companies in 2013 About Cyberattacks
Washington Post (03/25/14) Nakashima, Ellen

Federal agents reportedly notified more than 3,000 U.S. companies last year that their computer systems had been hacked. This marks the first time the federal government has revealed how often it tipped off the private sector about cyber-intrusions. The alerts were provided to companies of all sizes, including local banks, major defense contractors, and national retailers such as Target. However, the total reflects only a fraction of the true scale of such intrusions into the private sector by criminal groups and foreign governments and their proxies, especially in Eastern Europe and China. Analysts say that cybersecurity breaches cost American companies and consumers as much as $100 billion per year.

Profiles in Excellence

Gary S. Reynolds
Senior Vice President
Corporate Security and Director
Union Bank, N.A.

Editor's Note: In this issue, we highlight one of the Banking and Financial Services Council's newest members who will work as part of the Communications Committee. Welcome aboard Gary!

Mr. Gary S. Reynolds is the Senior Vice President and Corporate Security and Investigations Director for Union Bank, N.A., where he is responsible for the development of effective strategies to mitigate risk, maintain continuity of operations, and safeguard the organization by providing a physical and technically secure environment for employees, customers, and assets. He has established effective safety measures and developed crisis response plans for the Executive Protection Program. Gary is responsible for department policy and procedures development that meet regulatory and Bank requirements. He oversees and ensures that internal and external fraud and investigative activities achieve desired results while meeting the regulatory requirements of Bank Protection Act and the Bank Secrecy Act. Gary is Union Banks' primary liaison with the Bank of Tokyo Mitsubishi UFJ, Global Compliance Risk Department.

Prior to Union Bank, Gary was the Chief Security Officer for Dragnet Solutions, Inc., with responsibilities for business development, physical, and logical security. He led development teams that created innovative uses for facial recognition and identity management to unveil criminal behavior in real time.

Previous to joining Dragnet Solutions, Gary held the position of SVP/Director of Financial and Electronic Crime Investigations and Executive Protection at Wells Fargo Bank. With a team of 60 investigators, Gary headed all aspects of external fraud crimes aimed at the bank. He managed the electronic crime investigation team overseeing outsider/insider attacks, forensic investigations, and electronic discovery. Prior to joining Wells Fargo, Gary spent 20 years in law enforcement and is retired from the Santa Rosa Police Department.

Gary holds a B.A. degree from the University of Redlands, and a MS degree from Utica College of New York, where he is currently an adjunct professor teaching at the graduate level in the Economic Crime Management Program. He is also on the staff at the Santa Rosa Junior College Public Safety Training Center where he teaches Unusual Incident Management at the basic academy.

Gary is a Certified Fraud Examiner (CFE), Certified Anti Terrorism Specialist (CAS), and holds a Certificate in Computer Forensics from Oregon State University. He is a licensed private investigator and current member of the International Association of Bomb Technicians and Investigators. Gary was recently selected to serve on the ASIS, International Banking and Financial Services Council, and is on the advisory board of the International Association of Financial Crime Investigators.

Gary is a nationally recognized speaker on identity theft and financial crime. His speaking assignments have included, The California Identity Theft Summit, Federal Deposit Insurance Corporation Identity Theft Symposium, Federal Financial Institutions Examination Council Conference, IRS Identity Theft Roundtable, ING Identity Theft Conference, and the Ameriprise Identity Theft Conference.