ASIS Banking & Financial Services Council Newsletter

VOLUME 8, EDITION 3 JULY-SEPTEMBER 2014

ASIS News

ASIS 60th Annual Seminar and Exhibits, September 29-October 2, 2014

We're just a week away from the most exciting and influential security event of the year! If you haven't yet registered—don't miss out.

- Discover the latest innovations in security from 600+ exhibiting companies.
- Learn proven strategies and build your knowledge.
- Unlimited networking opportunities and top-flight special events provide an ideal peer-to-peer forum for making connections and building your professional network.
- 250 education sessions spanning all security disciplines and industry sectors.
- (ISC)² Security Congress.

ASIS Chapter Recognized for P# Excellence

The Matthew Simeone Award Committee has announced the 2014 Award for Public Private Partnership Excellence will be presented to the ASIS Puget Sound Chapter and their public partner, the King's County Prosecutor's Office.

Active-duty Military Receive Certification Scholarships

Congratulations to the five ASIS active-duty military members who received full ASIS board certification scholarships.

Information on Ebola Virus

Given the news' focus on this disease, ASIS has compiled resources on the subject, both information for the general public and data specifically targeted to those involved with healthcare.

Streamlined Wharton/ASIS Program to Launch in November

Learn how to keep security a top concern and budget priority in the newly redesigned program. It’s now more accessible and affordable.

Young Professionals Win First Seminar Experience

ASIS Young Professionals, in partnership with exclusive sponsor, Securitas Security Services USA, is pleased to announce the winners of the 2014 Seminar Experience.

Upcoming Programs and Webinars

October 15, 2014 (Webinar)

The Art and Science of Selling Security Guard Services

October 20-22, 2014

Video Surveillance Advancements and Case Studies

October 23-24, 2014

Risk, Threat & Vulnerability Assessment

October 27-28, 2014

Corporate Investigations: How to Conduct Proper and Effective Internal Investigations

October 29, 2014 (Webinar)

Budget and Finance Essentials for a Security Professional

October 29-30, 2014

The Investigative Interviewing Method

November 3-4, 2014

Executive Protection

November 3-6, 2014

ASIS Assets Protections Course: Principles of Security (APC I)

November 16-21, 2014

Wharton/ASIS Program for Security Executives

ASIS
BANKING &
FINANCIAL SERVICES
COUNCIL MEMBERS

IN THIS ISSUE:

In The News

375 Million Customer Records Compromised in 2014

07/30/14

This year has seen more than 375 million customer records lost to breaches worldwide, with the retail industry suffering more data losses than any other sector—145 million-plus records—in the second quarter, according to SafeNet's second-quarter Breach Level Index. SafeNet also found that less than 1 percent of all 237 beaches in the second quarter were secure breaches where strong encryption or authentication solutions shielded the data from exploitation. In addition, malicious outsiders were responsible for compromising 99 percent of the records and 56 percent of the breaches in the quarter. Moreover, the U.S. comprised 85 percent of records compromised globally and 74 percent of all reported incidents. The index also found that breaches against financial services declined substantially from the first quarter, from 56 percent to less than 1 percent of records compromised in the second quarter. "Businesses need to start thinking beyond plan A of 'how do I prevent a breach' and add a plan B which focuses on minimizing the impact of consumer data loss," says SafeNet's Tsion Gonen. "For example, using encryption to deem the data useless. It seems that if consumers don't start to demand that companies pay the price for these breaches, the current data breach epidemic likely will never end."

Behavior Patterns That Can Indicate an Insider Threat

08/07/14

Organizations that pay attention to the red flags that appear during the planning stages of insider threats such as trade secret theft, workplace shootings, and the sabotaging of information systems may be able to prevent these threats from being perpetrated. These red flags can take a variety of forms, including policy violations and poor job performance, and are different for each type of insider threat. The first step in preventing insider threats is to identify the warning signs that correspond to the threat or threats that the organization is most concerned with. Once these warning signs are identified, an organization can then begin collecting data on employees to see if any red flags are present. The data that is collected can take two forms: virtual data, or the types of digital trails that employees leave behind when they access the Web or internal IT resources; and non-virtual data, which includes information about the employee such as performance ratings, compliance with policies, and data on physical movements within the office. Both of types of data can then be fed into analytic tools that can identify behavior that deviates from certain norms. However, organizations must also rely on other methods for preventing insider threats, including implementing policies, procedures, and controls for protecting assets whose security may be threatened by malicious insiders.

Arab Bank in Court Over Accusations it Helped Funnel Money for Terrorism

08/15/14

The Jordan-based Arab Bank funneled tens of millions of dollars to the families of militants with ties to Hamas during a Palestinian uprising that took place from 2001 to 2004, according to lawyers for American terror victims. In a federal trial in Brooklyn, attorney Tab Turner said that cash was distributed to relatives of dead bombers at bank branches in the West Bank and Gaza, and that the bank officials "knew these neighbors of theirs were evil and criminal people." Arab Bank attorney Shand Stephens argued that Arab Bank had followed regulations for screening transactions against lists of known terrorists, and that the bank was following instructions from the Saudi Committee for Supporting Al Quds intifada, an organization run by Saudi Arabia. a benefit plan for martyrs.

ASIS INTERNATIONAL
Advancing Security Worldwide®

In The News

OSHA is Cracking Down on Workplace Violence. Are You at Risk?

08/18/2014

Although the Occupational Safety and Health Administration (OSHA) does not have a specific workplace violence standard, it recently cited two employers for failing to protect their workers from threats and assaults. OSHA reports that delivery drivers, healthcare professionals, public-service workers, customer-service employees, and law-enforcement employees are at higher risk for workplace violence. Risk factors include exchanging money with the public; working with volatile, unstable people; working in isolated conditions or late at night; and working in areas with high crime rates or where alcohol is served. OSHA recommends that organizations protect employees from workplace violence by using administrative controls, such as job site hazard assessments and incident reviews; engineering controls, such as panic alarm systems and protective barriers; personal protective equipment, such as personal alarm systems for staff; and training that includes workplace violence prevention and stress management, as well as post-incident services.

New Industry Group Tackles ATM Fraud

08/20/14

ATM manufacturers Diebold and Wincor Nixdorf are laying the groundwork for the formation of a new global industry group focused on thwarting ATM crime. The aim of this group is to establish industrywide technical standards for secure ATM terminals and ATM components and provide a platform for information sharing about attack scenarios and emerging threats, said Joerg Engelhardt, vice president of global product management for Diebold.

Credit-Card Industry Ramps Up Security Efforts

09/05/14

In response to a rash of data breaches at major U.S. retailers, the credit-card industry is accelerating efforts to keep sensitive customer information out of the hands of merchants. Visa and MasterCard are rolling out technology that replaces cardholder information such as account numbers and expiration dates with a unique series of numbers that validates the customer's identity. Called "tokenization," the new technology can be used for online transactions, payments made in a physical store with a smartphone, and with merchant applications that consumers load onto a smartphone. By getting rid of the sensitive card information, banks and merchants can leave hackers with nothing of value to steal if they break into their computer servers. "There is a recognition that we all need to evolve the payment standards to embrace what is going on around us," says Jim McCarthy, Visa's global head of innovation and strategic partnerships.

OSHA is Cracking Down on Workplace Violence. Are You at Risk?

08/18/2014

Although the Occupational Safety and Health Administration (OSHA) does not have a specific workplace violence standard, it recently cited two employers for failing to protect their workers from threats and assaults. OSHA reports that delivery drivers, healthcare professionals, public-service workers, customer-service employees, and law-enforcement employees are at higher risk for workplace violence. Risk factors include exchanging money with the public; working with volatile, unstable people; working in isolated conditions or late at night; and working in areas with high crime rates or where alcohol is served. OSHA recommends that organizations protect employees from workplace violence by using administrative controls, such as job site hazard assessments and incident reviews; engineering controls, such as panic alarm systems and protective barriers; personal protective equipment, such as personal alarm systems for staff; and training that includes workplace violence prevention and stress management, as well as post-incident services.

New Industry Group Tackles ATM Fraud

08/20/14

ATM manufacturers Diebold and Wincor Nixdorf are laying the groundwork for the formation of a new global industry group focused on thwarting ATM crime. The aim of this group is to establish industrywide technical standards for secure ATM terminals and ATM components and provide a platform for information sharing about attack scenarios and emerging threats, said Joerg Engelhardt, vice president of global product management for Diebold.

In The News

Credit-Card Industry Ramps Up Security Efforts

09/05/14

In response to a rash of data breaches at major U.S. retailers, the credit-card industry is accelerating efforts to keep sensitive customer information out of the hands of merchants. Visa and MasterCard are rolling out technology that replaces cardholder information such as account numbers and expiration dates with a unique series of numbers that validates the customer's identity. Called "tokenization," the new technology can be used for online transactions, payments made in a physical store with a smartphone, and with merchant applications that consumers load onto a smartphone. By getting rid of the sensitive card information, banks and merchants can leave hackers with nothing of value to steal if they break into their computer servers. "There is a recognition that we all need to evolve the payment standards to embrace what is going on around us," says Jim McCarthy, Visa's global head of innovation and strategic partnerships.

“Active Shooter” Drills Spark Raft of Legal Complaints

09/04/14

"Active shooter" drills have become increasingly common in schools and workplaces following a series of high-profile mass shootings in recent years. At least five states have put in place new laws requiring schools to carry out active shooter drills in addition to and separate from disaster preparedness drills. However, the companies and police departments that carryout these drills are increasingly finding themselves on the receiving end of legal action from employees who say the drills are too lifelike or uncontrolled, leaving participants too traumatized, and in some cases actually injured, to learn anything. One major complaint is that employees are sometimes not informed that the drills will be happening and mistake them for the real thing. A nurse at a Colorado nursing home is suing a police officer and her employer after a drill that left her so traumatized she had to quit her job. Other times the drills get out of control and people get hurt. An Ohio man filed a lawsuit after he was unexpectedly tackled by a police officer during an active shooter drill, resulting in serious injuries to his hip and shoulder. "There ends up being zero learning going on because everyone is upset that you've scared the crap out of them," former SWAT team member Greg Crane says of such shooter drills.

Homeland Security: 'No Evidence' ISIS Will Cross U.S. Border

09/16/14

Homeland Security officials are working to counter persistent claims from conservative groups and politicians that agents of the Islamic State (IS) either are attempting or have already crossed the border into the U.S. from Mexico. Those making such claims include Texas Gov. Rick Perry and Sen. Ted Cruz (R-Texas), who said in a recent op-ed piece that, "the government is making it too easy for terrorists to infiltrate our nation." Rep Ted Poe (R-Texas), meanwhile, has

Rep Ted Poe (R-Texas), meanwhile, has

theorized that IS agents could partner with drug traffickers to sneak into the U.S. across the southern border. On Monday, a Texas sheriff claimed that a copy of the Koran and "Muslim clothes" were found along the border, presenting this as proof that "Muslims ... have been smuggled in the United States." On the same day, the Department of Homeland Security said that there is no credible evidence backing up claims that IS is actively planning to infiltrate the U.S. across the southern border. Rep. Robert O'Rourke (D-Texas) says that claims about terrorists crossing the southern border are not new and were not correct when they centered on al-Qaida and Iranian agents either.

ASIS Announces Accolades Award Winners

09/17/14

ASIS International has announced the winners of its 2014 Accolades Awards, which recognize innovative security products, services, and solutions. This year's winners were chosen by a panel of judges representing end users and security experts and will be presented at ASIS' upcoming conference in Atlanta on Sept. 29.

Cyber Security

Network Security Concerns With BYOD
08/04/14

The analyst firm Ovum says close to 70 percent of employees use personal tablets or phones to access corporate data. Twenty-one percent do so despite an established policy, and 15.4 percent do so without the knowledge of their IT departments. While experts say banks increasingly are accepting that Bring Your Own Device is here to stay, not all banks are testing their networks to identify potential security problems that might arise from BYOD. Despite the risks, BYOD can lower equipment costs, boost productivity and response times, and enhance employee engagement. However, network protection is critical, given that banks can lose millions of dollars if malicious traffic shuts down or even slows their networks. Experts note that banks cannot employ remote wiping of personal devices, nor can they expect a complete ban on BYOD to succeed. Thus, it is important for banks to test their networks by simulating breach attempts and needle-in-a-haystack scenarios, and these tests should be comprehensive and continuous and include the latest applications and updated malware definitions. Moreover, experts say banks should establish BYOD policies that balance security needs with employee productivity and mobility.

Data Breaches and High-Risk Vulnerabilities Continue to Dominate
08/12/14

There have been more than 400 data breaches this year through July 15, resulting in more than 10 million personal records being exposed, according to Trend Micro. Customer names, passwords, email addresses, and birthdates were among the different types of information exposed in some of the breaches. The report also notes the severity and volume of attacks is on the rise, underscoring the need for organizations to engage in incident response planning and carry out security awareness initiatives that aim to educate all their employees. Trend Micro also offers several other recommendations for how organizations can improve cybersecurity in the face of a growing number of increasingly sophisticated cyberattacks. Trend Micro's Raimund Genes says organizations need to take a more comprehensive approach to cybersecurity, particularly by integrating their cybersecurity strategies into their long-term business strategies instead of simply handling security issues as "tertiary, minor setbacks." Meanwhile, Trend Micro's JD Sherry calls on organizations to take a collaborative approach involving both internal and external stakeholders to amass the resources they need to protect themselves from cyberattacks and respond to any attacks that may take place.

Cybersecurity Threats Demand Small-Bank Directors' Attention
08/28/14

With data breaches against retailers and other companies on the rise, community bank directors are becoming more involved in cybersecurity matters. However, experts say boards need to focus on governance as it relates to cybersecurity, rather than get involved in decision making. Sage Data Security founder Sari Stern Greene says, "The foundation of the bank-customer relationship is trust. It is the responsibility of the institution to honor that trust and that emanates from the top." Greene says directors could learn about ransomware trojans, for instance, then ask management questions about preparedness, and they should ensure the bank tests its security and reviews its policies on an annual basis. With regulators calling on banks to increase their oversight of third-party lenders, directors also should ensure contracts with third parties protect the bank in the event of a breach and perform due diligence on the subcontractors used by their vendors. At the $1.6 billion-asset Northwest Financial in Arnolds Park, Iowa, for instance, directors are given quarterly updates on technology projects and engage in big-picture discussions about security.

Why Info-Security Hinges on Physical Security
09/14/14

Headline-grabbing data breaches have emphasized the need for logical security of computers and mobile devices, but physical security remains an important defense layer. A combination of different types of controls, often called "defense-in-depth," is vital for the protection of data and devices. Security expert Michael S. Oberlaender points out that some data centers are located in shared facilities with other companies, and are not fully secured from physical intrusion. authentication, and the use of strong passwords.

ASIS Foundation Offers Significant Resources

Richard E. Widup, Jr.,CPP

ASIS 2014 President

Just last month, five active duty military members received full certification scholarships to support their efforts to earn CPP and PSP security certifications. This is just one of the many scholarship programs offered by the ASIS Foundation, whose mission is to "provide actionable research and scholarship opportunities to enhance and advance the security profession."

Full tuition scholarships (market value of $180,000 to $270,000) were awarded this year to 10 security practitioners from around the world to pursue undergraduate and graduate degrees at the University of Phoenix and Webster University, and prizes totaling $3,500 will be awarded to four undergraduate and graduate students for outstanding papers on security issues. These programs—that help individuals pursue education, certification and research make me proud of my membership in ASIS.

The Foundation supports the profession in numerous ways, giving a helping hand to the security leaders of tomorrow. As an association, we must care about the future of our profession—the ASIS Foundation is our vehicle for doing so.

In addition to scholarships, the Foundation recognizes excellence in action today and thereby encourages future good work.

At ASIS 2014, I look forward to meeting members from the ASIS Puget Sound Chapter—the recipient of the 2014 Matthew Simeone Award for Public Private Partnership Excellence. The public-private partnership tackled a major problem of organized retail crime that was causing economic devastation to retailers in Washington State.

The Piedmont chapter will benefit from two days of a physical security education program thanks to the Roy Bordes Award for Physical Security, which the chapter won this year for their efforts to expand membership and educational offerings.

Research is a major focus for the ASIS Foundation, which commissions industry, academic, and government thought leaders to research security challenges and issues. This year the Foundation released a study on security metrics and a companion tool that security professionals can self-administer to develop, evaluate, and improve security metrics within their organization. Persuading Senior Management with Effective, Evaluated Security Metrics is the culmination of a year-long research project funded by the ASIS Foundation.

Key findings from a national roundtable and a broader survey of 3,000 security practitioners to examine top security risks and necessary competencies for security professionals was published recently in Security Industry Survey of Risks and Professional and Professional Competencies.

Think about the gaps in industry knowledge that would exist without these Foundation- supported research projects and publications!

Attendees of ASIS 2014 have the opportunity to support this work by purchasing tickets for themselves, staff, clients, and colleagues to attend the Foundation's two signature fundraising events—the annual golf tournament and Foundation Night.

Kickoff your Seminar week at the Golf Tournament, Sunday, September 28, at the Stone Mountain Golf Club and then wind down at Foundation Night on Wednesday, October 1, at Der Biergarten in downtown Atlanta. If you cannot attend, please consider becoming a 'Friend of the Foundation' by making an online donation.

These are just a few highlights of the remarkable work done by the ASIS Foundation. How can we possibly advance the security profession without investment in programs such as these? We can't and therefore I hope that you will take up my challenge by attending Foundation events or making an online donation.

ASIS INTERNATIONAL
Advancing Security Worldwide®