ASIS Banking & Financial Services Council Newsletter

VOLUME 8, EDITION 2 APRIL-JUNE 2014

ASIS News

ASIS Foundation Releases Security Performance Metrics Study

Metrics are vital when it comes to presenting a sound, compelling proposition to senior management for security enhancements. However, until now, there has been relatively few tested metrics and little guidance.

The ASIS Defense and Intelligence Council and the ASIS Foundation are pleased to announce the release of Persuading Senior Management with Effective, Evaluated Security Metrics, an in-depth research report based on actual case studies of effective metrics in use by practitioners.

The report offers:

- The Security Metrics Evaluation Tool
- A Library of metric descriptions
- Guidelines for effective use of security metrics

Get started now - increase the quality of your assessments and demonstrate the value of your security plans to senior management with proven metrics.

Download your FREE copy from www.asisfoundation.org.

Young Professionals Win a Seminar Experience

ASIS Young Professionals, together with exclusive sponsor Securitas, is offering young professionals (YP) the opportunity to win one of three Seminar Experiences. Each winning YP will receive a full conference registration, travel voucher, housing, and networking event tickets. Deadline is 31 July!

Join us in Atlanta, Georgia, September 29–October 2, 2014 for the ASIS International 60th Annual Seminar and Exhibits—the world's most influential security event.

Program highlights include:

- 250 education sessions spanning all security disciplines and industry sectors
- Security products and services from 600+ leading solutions providers
- Unmatched peer-to-peer networking opportunities
- Collocated event: (ISC)² Security Congress.

Upcoming Webinars

July 14-15
Executive Protection

July 14-17
Managing your Physical Security Program: An Advanced Workshop for Managers and Practitioners

July 16 , 2014
Twelve Symptoms of a School with Problems

July 16-17
Security Program Design: A Critical Infrastructure Protection Model

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

Report: Growing Risk of Cyber Attacks on Banks
Associated Press (05/06/14)

New York Gov. Andrew Cuomo and the state's Department of Financial Services issued a report on May 5 warning that cyber thieves are using increasingly sophisticated methods to breach bank accounts. A yearlong survey of New York bank security found that a majority of the 154 banks surveyed reported being the target of cyber attacks in the past three years. The attacks involved the use of malicious software and phishing schemes intended to take over bank accounts, seize data, and steal the identity of bank customers. Cuomo says he is directing bank regulators to regularly analyze bank security practices to determine how vulnerable they are to attack.

Data Breaches: A New Source of Worry for CEOs
Associated Press (05/06/14)

Data breaches can be used to cast blame on CEOs, as indicated by Target CEO Gregg Steinhafel's ouster this week. "Ultimately, it's the CIO and the IT managers that are really more in the weeds," says FBR Capital Markets analyst Daniel Ives. "But just like the head coach of a football or basketball team that doesn't make the playoffs, the CEO is ultimately responsible." Virginia Commonwealth University Professor Ronald Humphrey thinks that although the CEO is responsible for data security, the issue is often overlooked since it is not always identified as a key operational component. "This is a wakeup call to CEOs that data security is something that affects their customers," he notes. "If you've had your identity stolen you know it's a huge headache. I think they have to take this very seriously." Humphrey also says in the event of a breach, a CEO must be able to show the board of directors that it did not stem from a dearth of resources committed to data security.

Researchers discover critical flaws in the Chip and PIN system

Help Net Security (05/19/14)

Researchers at Cambridge University identified two vulnerabilities in the Europay, MasterCard, and Visa (EMV) 'chip and PIN' payment card system that could allow attackers to carry out "pre-play" attacks in order to commit ATM or point of sale (POS) fraud. One vulnerability involves poor random number generation that could be predicted and used for ATM withdrawal, while the second is a protocol failure that could enable malware or a man-in-the-middle (MitM) attack to replace randomly generated numbers with ones chosen by the attacker.

Security Guard Industry Lacks Standards, Training
MSUToday (06/03/14)

A study by Michigan State University criminologists that was published in Security Journal has found that many states lack adequate training standards for security guards. Though the number of security guards has increased to more than 1 million, the study found that states have not strengthened the minimum standards and training requirements for those who fill these positions since 1982. The study also found that many states completely lack training standards, while others do not set requirements for minimum education levels or require background checks for security guards. The lack of training standards forces guards to learn on the job if their employers do not provide training. A second study by MSU researchers interviewed security officers and found that they largely feel that they are unprepared to handle physical altercations and problematic individuals or even to protect themselves due to a lack of training. However, the study found that some guards are able to draw on their backgrounds as police officers. Additionally, the interviews revealed that security guards are strongly in favor of introducing standardized, systemic training for the industry.

In The News

The Business of Travel Safety
Security Management (06/14/14)

Businesses must take steps to protect employees when they travel abroad, writes Tzviel Blankchtein, the operator of Masada Tactical Protective Services. Kidnappings and hostage situations remain a serious threat for traveling executives, he maintains, and companies should be prepared for worst case scenarios. Blankchtein says any employee sent to a high-risk area should be protected via planning, training, tracking, and preparing for emergency procedures. In the planning stage, a thorough risk assessment should be performed to identify the modes of travel and the safest routes to use as well as risks posed by lodging options and social climate. If possible, a security team should be sent in advance of the trip to better assess these risks. This information should be used to prepare executives during a pre-travel training session. Such training will also help teach executives to blend in by adopting to local customs so they do not appear to be high-value targets. Training may additionally help executives learn simple self-defense techniques and familiarize them with their company's emergency protocols. Even with this information, it is important for companies to be able to track executives, which can help identify a kidnapping situation and speed recovery operations. Finally, should a kidnapping occur, the company must have emergency procedures in place to increase the executive's chances of a safe return.

Workplace Violence Prevention Starts with Comprehensive Employee Training
Business Insurance (06/08/14)
Workplace violence education is an essential part of employee training because it teaches staff to detect and report potential threats and respond to those that materialize as safely as possible. Employees should be made aware of their company's emergency response procedures, including communication protocols, evacuation routes, and local law enforcement plans. Preparedness also involves being aware of the signs that someone may be contemplating committing an act of violence and taking action when those red flags are seen. "I've never encountered a situation where there hasn't been 20 different signs that something was going to happen. A lot of people knew about it, but they didn't know what to do, so they didn't take action," said Dr. Teresa Bartlett, the senior vice president of medical quality at Sedgwick Claims Management Services Inc. The way a company chooses to convey such information is important as well. For example, some may elect to use computer-based workplace violence reporting systems that provide information about potential warning signs, such as extreme emotions, erratic behavior, or isolation.

Companies Can Spend Millions on Security Measures to Keep Executives Safe
Chicago Tribune (06/08/14)

Many defense contractors and large corporations are reportedly spending hundreds of thousands of dollars a year ensuring their top executives are safe. This trips. Such top defense contractors as Lockheed Martin cite threats passed on from government agencies and law enforcement as reasons for these expenditures.

Ex-FBI Boss Urges Tougher Corporate Security
San Antonio Express-News (06/17/14)

At the annual Global Fraud Conference in San Antonio, Texas, on Monday, former FBI Director Louis Freeh said that financial institutions and other companies may soon need to improve their internal defenses against intellectual property theft. Freeh, who is now the CEO of Freeh Group International Solutions, commented that the Securities and Exchange Commission (SEC) will be looking for guidance that will be used to aid financial institutions in explaining their intellectual property protections. He encouraged companies to implement stronger security measures to protect their intellectual property, adding that protecting intellectual property is critical to the country's economic and national security. Freeh added that copyright and patent infringements already cost an estimated hundred of billions of dollars each year.

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

Web Attacks, ATM Skimming Top Banks' Security Threat List: Report
Bank Technology News (04/22/14)

The Target card data breach dominated headlines last year, but it was just one of hundreds of hacking incidents to hit banks and expose the personal information of their customers, according to Verizon's latest Data Breach Investigations Report. The biggest security threats to banks last year were web app tampering, distributed denial-of-service attacks, and the increased use of payment card skimmers, according to Verizon's widely trusted report, which was released Monday. These three categories of attacks made up three-quarters of security incidents targeting banks. Verizon, with the help of 50 partners including law enforcement agencies, the Financial Services-Information Sharing and Analysis Center, government agencies, other forensic investigation companies, and research companies, tracked 1,367 confirmed data breaches and 63,437 security incidents in 95 countries. More than one-quarter — 27% — of all security breaches at banks last year involved web app attacks, the report found. In web app attacks, cybercriminals use a variety of tactics to interfere with web applications. Many start with phishing, a fake email sent to a customer that appears to be from their bank that tricks them into sharing their user name and password, or into clicking on a link that leads to the installation of malware on their machine. Brute-force password guessing can also be used in a web app attack. A less-used type of web app attack uses SQL injection, in which a hacker inserts malicious SQL statements into an entry field for execution; for instance, to dump the database contents to the attacker. (Distributed denial-of-service attacks can also be web app attacks, but due to the volume and impact of DDoS, Verizon broke those out separately.)

Microsoft Study Says Cyber-Criminals Resort More to Deceptive Measures
eWeek (05/07/14)

The latest Security Intelligence Report from Microsoft's Trustworthy Computing division says that although Microsoft software is much more resistant to remote-access exploits than in recent years, attackers are compensating by using "deceptive tactics" to install malware on target systems. Tim Rains, director of Trustworthy Computing, says there has been "a 70 percent decline in the number of severe vulnerabilities [those that can enable remote code execution] that were exploited in Microsoft products between 2010 and 2013." However, Rains says the second half of 2013 saw "a noticeable increase" in the use of deceptive practices, such as hiding malware and ransomware in seemingly legitimate downloads. Malware infections due to deceptive tactics nearly tripled in the last quarter of 2013, according to Rains. Another tactic being used is delaying the deployment of a malware payload once it is inside a target system. There also were hints that different attackers were coordinating their efforts, with a Microsoft spokesperson reporting three of the top 10 malware families—Rotbrow, Brantall, and Sefnit—have been known to work together.

Money, Skills, and Hired Guns: 2014 Strategic Security Survey
InformationWeek (05/12/14)

The findings of CounterTack's 2014 Strategic Security Survey reveal a number of challenges and trends likely to shape enterprise information security in 2014. Although there was little sign that the quality or investment in IT security is declining, there also was little sign of forward momentum. Nearly 25 percent of respondents said their organization had been the victim of a data breach or some form of cyberespionage in the last year. Asked what contributed to their vulnerability, 40 percent cited budget constraints, compare to only 30 percent in 2013. More than three-fourths also pointed to the increased sophistication of attacks and more than two-thirds to increasingly vulnerable networks. CounterTack's Michael Davis says one of the key issues identified by the survey was that most IT security systems are judged not by how successful they are at thwarting attacks, but by how well they perform on compliance checklists. Going forward, Davis says this compliance mindset and budget pressures are likely to result in more medium and small enterprises turning to third-party providers to meet their comprehensive security needs.

The Indispensable Work of ASIS

Richard E. Widup, Jr.,CPP
ASIS 2014 President

In my June column, I mentioned the release of an extremely valuable "how to" guide for developing goal-oriented public-private partnerships, prepared by the ASIS Law Enforcement Liaison Council (LELC). Well, the LELC did not stop there. Building on the theme of the new guide, the group also has developed a timely education session for the upcoming ASIS Seminar and Exhibits: "Cyberfraud: How to Protect Yourself and Your Business." A panel of public/private industry experts who deal with cyber threats on a daily basis will examine the current threats and discuss why working together is the key to any incident response.

The LELC is one of our 29 professional councils—each focusing on a specialized security practice area, from Academic and Training Programs to Utilities Security. This is one of the most valuable and most practical benefits of an ASIS membership, in my opinion.

These 29 councils form the nerve center of the security profession, developing best practices, collaborating on common issues, and identifying emerging industry trends in these security niches. Indeed, 22 of the 29 councils have developed education sessions for ASIS 2014.Fifty-four sessions—more than 25% of the programs offered this year—are sponsored by ASIS councils. Several councils are presenting more than one education session; in fact, three of them—Information Technology Security Council, Defense and Intelligence Council, and Physical Security Council—will offer five or more sessions in Atlanta.

The 54 council-sponsored sessions will cover a wide range of security issues, providing insight and solutions that attendees can take back to the office. For example, "Seeing is Believing: Better Situational Awareness Through Video Quality in Public Safety," presented by the Physical Security Council, will review the exponential increase in video technology and explain how to navigate the staggering number of product choices on the market today.

Are you responsible for securing energy industry ports and maritime assets? Don't miss the Petrochemical, Chemical, and Extractive Security Council session "Securing Energy Industry Port and Maritime Assets: The Dynamics of International Operations". Most of us will be affected one way or another by the Affordable Care Act's employer mandate that takes effect on January 1, 2015. Thanks to the Women in Security Ad-hoc Council, we have this important session: "2015 Affordable Care Act: Impact on the Security Services Industry Make the Case for Wellness".

You can see why ASIS Councils are indispensable, they have the expertise to go deep into a topic and the desire to share their knowledge with their peers, whether it is for the annual Seminar and Exhibits, classroom programs or other ASIS educational offerings. They are our "go to" people when only the best in these particular specialties will do. ASIS councils continue to expand and excel for another reason; they are excellent networking opportunities. I often hear from council members how much they value the camaraderie that is a natural outcome of working side-by-side on special projects and making decision together. Leadership skills are built and fine-tuned on ASIS councils as well.

I urge all members to consider joining a council. With so many to choose from, there surely is a good match for every member.