ASIS Banking & Financial Services Council Newsletter

VOLUME 8, EDITION 4 OCTOBER-DECEMBER 2014

ASIS News

ASIS International Presents Inaugural Security Book of the Year

ASIS International honored author Michael Jay Fagel, PhD, CEM, CHS-IV, with its inaugural Security Book of the Year Award on Mon., Sept. 29, at the ASIS International 60th Annual Seminar and Exhibits, held in Atlanta, Ga. Fagel's award-wining book, "Crisis Management and Emergency Planning: Preparing for Today's Challenges" was published in 2014.

"The investment of time and talent by book authors and editors is enormous. ASIS has long worked closely with many authors and editors. I felt strongly that there was a need to recognize their commitment and achievement among their peers and within their profession," stated Lawrence J. Fennelly, CPO, CSS, author and editor of more than 30 security books, who worked with ASIS to establish the award and chair the inaugural award committee.

Dr. Fagel has more than three decades of experience in emergency management and emergency operations. He has been an on-site responder to such disaster events as the Oklahoma City Bombing and the site of the World Trade Center in the aftermath of 9/11. He is an experienced professor, trainer, and consultant and has pretty much seen it all.

Thank you for attending ASIS 2014

Thank you to the thousands of exhibitors, attendees, and speakers, who joined us in Atlanta for the 60th ASIS International Annual Seminar and Exhibits, September 29-October 2. We appreciate your support and look forward to seeing you in Anaheim for ASIS 2015!

Reminder: CPE Policy Updates Effective January 2015

Effective January 2015, CPPs, PCIs, and PSPs will be required to earn 60 CPEs every three years.

School Security Webinar and Best Practices in ASIS security Spotlight

The ASIS Law Enforcement Liaison Council has awarded the 2014 Matthew Simeone Award for Public Private Partnership Excellence to the ASIS Puget Chapter.

ASIS Launches Digital Credentials

The ASIS Professional Certification Board is pleased to announce the launch of digital credentials.

Upcoming Programs and Webinars

January 28, 2015

Trends and Technology Driving Change in Security Insights from the Latest Industry Research and Data

February 2-3, 2015 (Webinar)

Viewpoints in Health Care Security: Achieve Success in Today's Healthcare Environment

February 15-17, 2015

ASIS 6th Middle East Security Conference & Exhibition

February 23-24, 2015

PSP Review Program

February 23-24, 2015

CPP Review Program

February 23-24, 2015

Physical Security Introductory Applications and Techniques

February 25-26, 2015

Security Documents and Project Management Process

March 16-19, 2015

ASIS Assets Protection Course:

Principles of Security (APC I)

March 29-31, 2015

ASIS 14th European Security Conference & Exhibition

IN THIS ISSUE:

In The News

How Companies Blow it With Security Breaches
The Wall Street Journal (10/31/14)

McKinsey & Co. Global Managing Director Dominic Barton said he sees three common mistakes companies make when they have a security breach. The first is an inability to make efficient decisions. Barton said organizations should have a plan before a security breach happens and if companies wait until a breach to do so, they end up designing their response plan when emotions and pressure are elevated. The second mistake is the failure to communicate about the breach to the right set of stakeholders in the right way. He said organizations either tend to share too much or too little information with customers. In addition, what breached companies tell regulators may sometimes be different than what customer service representatives are telling customers. Last, he sees a hesitancy to adjust business strategies in the wake of the breach. Barton said companies need to look past the immediate IT remediation and evaluate the impact on business strategy and core operational process.

Americans Top Fear: Credit Card Data Getting Stolen
Pymnts.com (10/29/14)

U.S. adults say their top fear is having their credit card data stolen by cyber thieves, according to a new Gallup poll. About 69 percent of those surveyed said they feared credit card data attacks, followed by 62 percent citing cyber thieves hacking into their desktop computer or smartphone and stealing private data. The survey marks the first year that Gallup included the theft of credit card information or having a smartphone attacked. "Upper-income Americans, those whose household incomes are $75,000 or more a year, are more likely than lower-income Americans to worry frequently or occasionally about hacking of their credit card information, 85 percent to 50 percent," Gallup says. "Americans between the ages of 30 and 64 worry about this more than younger and older Americans do."

Security Firm Predicts Hackers Will Target Apple Pay and ATMs in 2015
DigitalTransactions.net (12/02/14)

Apple Pay will be a target of cybercriminals in the coming year, according to predictions from Kaspersky Labs. Apple's increasing market share makes its recently released mobile wallet app an enticing target for hackers, says Kaspersky researcher Patrick Nielsen. "It really doesn't have that much to do with the security of the platform," he says. Apple Pay offers far more security than magnetic-stripe payment cards with its combination of NFC technology, tokenization, and fingerprint biometrics.

The Well-Vetted Workforce
Security Management (12/14/14)

Experts say that comprehensive corporate security programs need to focus on protecting the company from problem employees, because hiring the wrong person can easily become a liability or security threat. Recruitment must be done properly in order for the hiring process to be quick and efficient. Employment history and education are one of the most important components in a resume, thus verifying institutions attended and degrees received helps ensure the applicant's honesty. Data shows that almost one-third of employers do not check employment records. Drug testing is essential because workplace drug use creates an unsafe work environment. Drug testing can also help increase productivity and decrease absenteeism. A study issued by the Society for Human Resource Management found that after drug testing was enforced, 19 percent of organizations reported an increase in productivity and 50 percent saw a decrease in absenteeism.

Cyber Security

Internet Experts: 'Widespread Harm' Likely From Cyberattack in Next Decade
Philadelphia Inquirer (PA) (10/30/14)

The Pew Research Center and Elon University's Imagining the Internet Center recently conducted a survey of more than 1,600 computer and Internet experts on the future of cyberattacks and found most respondents believe there is a significant threat. More than 60 percent of respondents think that by 2025, a major cyberattack will have caused widespread harm to a nation's security and capacity to defend itself and its people. "The majority opinion here is that these attacks will increase and that lots of institutions, including major government institutions, will be at risk," says Pew Research Internet Project director Lee Rainie. Although some experts think a Cold War-like dynamic of mutually assured destruction will inhibit international cyberwarfare, others see more danger to financial systems than to other essential infrastructure. Meanwhile, others say the threats themselves "are being exaggerated by people who might profit most from creating an atmosphere of fear," says Elon University researcher Janna Anderson. "While, in principle, all systems are crackable, it is also possible to embed security far more deeply in the future Internet than it is in the present Internet environment," says Syracuse University professor Lee McKnight.

States, U.S. Beef Up Cybersecurity Training for Bank Examiners
Wall Street Journal (11/30/14)

As financial institutions face increased threats from hackers, federal and state regulators are planning to boost cybersecurity training for bank examiners. The regulators also intend to hire IT experts to analyze how well banks are prepared for cyberthreats. Examiners have long been concerned about cybersecurity, but the issue has become more important after a series of incidents that include last summer's data breach at JPMorgan Chase. New York's Department of Financial Services, for example, plans to issue guidance about the way it conducts cybersecurity reviews of regulated financial institutions. The department will also hire a company to provide intensive training to its examiners and other staffers who work on IT issues. The Office of the Comptroller of the Currency, meanwhile, is training more staff in "operations risk," and the Federal Reserve is providing training that will give its examiners more IT expertise. The Conference of State Bank Supervisors is helping to arrange a cybersecurity summit for senior regulators and bank officials in Austin this week. This program is expected to be repeated throughout the United States next year.

The Persistent Threat of Data Breaches
Help Net Security (12/01/14)

Experian Data Breach Resolution's Michael Bruemmer says the recent rash of data breaches has made it more important than ever for organizations to prepare for cyberattacks. However, many companies may be neglecting to update their data breach response plans on a regular basis. Bruemmer says a recent survey found 41 percent of respondents had no established time period in place for reviewing and updating data breach response plans, while 37 percent said they had not reviewed or updated their plans since they were created. In addition to being prepared for data breaches, organizations also must be aware of the potential security risks created by the Internet of Things, says Experian's Ozzie Fonseca.

Computing Goes to the Cloud. So Does Crime.
New York Times (12/02/14)

As the influence and market share of cloud computing and storage have expanded, the cloud has inevitably become a major target for cybercriminals. IBM's Marc van Zadelhoff characterizes the battle with cybercriminals as "hand-to-hand combat." He notes IBM itself routinely receives taunting messages from Russian hackers seeking to steal from the hundreds of banks that IBM serves. Attacks on cloud systems range from the high-profile, but relatively low-tech attacks that resulted in the public release of several celebrities' personal photographs stored on public clouds, to more sophisticated and stealthy attacks targeting the financial and tech sectors. The cloud also has changed the sorts of attacks launched by cybercriminals. Numerous demonstrations have been made of how the cloud can become a tool, not just a target, for hackers. Compute time on cloud systems can be used to crack passwords and encryption or to build cloud-based botnets. However, the IT security industry is responding to this changing threat landscape with new tools and security solutions, ranging from improved systems diagnostics and monitoring to tools that seek to predict and actively mitigate attacks on cloud systems.

What a Year

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

As 2014 draws to a close, it is fitting to reflect on the achievements over the past 12 months while looking ahead to the future. I feel tremendous pride in my service as your president and in all we have accomplished together. I am also excited by the energy and momentum going into 2015.

Our support of professional development was clearly front and center this year with the launch of our webinar subscription series. This popular offering allowed members to earn CPEs, remain current on emerging security threats, and learn best practices from experts in their fields. Also significant were the debut of the AMU/ASIS Business Essentials for the Security Executive online graduate certificate program and a revamped Wharton Security Program.

ASIS rolled out two certificate programs—the Executive Protection certificate and the ASIS Assets Protection Course Principles of Security certificate. In 2015, three more certificate courses will be launched: Physical Security, Corporate Investigations, and Assets Protection Course Practical Applications.

In a productive year for our Standards and Guidelines program, thre ANSI standards were released: Chief Security Officer: An Organizational Model; Auditing Management Systems: Risk, Resilience, Security, and Continuity-Guidance for Application; and Supply Chain Risk Management: A Compilation of the Best Practices. Asis is leading the American effort on the international standard, ISO/PC 284, which will be the first to address managing risks to security operations while protecting human rights. In the year ahead, we also expect to conclude work on the much-appreciated ASIS/RIMS Risk Assessment standards as well as an investigation standard.

The ASIS Foundation continued to advance leading edge research and educational opportunities. This year two exceptional reports were released: Persuading Senior Management with Effective, Evaluated Metrics and The Security Industry Survey of Risks and Competencies. Both are available as free downloads. The Foundation was also awarded a record number of scholarships including 10 full tuition scholarships to the Univeristy of Phoenix and Webster Univeristy (valued at $200K+).

Another highlight has been the continued growth of our Women in Security and Young Professionals communities. These member-driven groups really took off this year and I am proud to announce they will become Councils in 2015.

As we prepare for the 60th anniversary of our society and I transition into my role as chairman of the board, I am more excited than ever before for the future. From the selfless dedication of our volunteer leaders to our organization's commitment to expanding education and professional development opportunities, I believe our best days are yet to come.

I want to say Thank You for such an enjoyable, productive, and memorable year. It has been my honor and privilege to serve as your president. On behalf of ASIS, I wish you all a happy, healthy and prosperous New Year.