ASIS Councils NEWSLETTER

Banking & Financial Services Council April—June 2012

Special points of interest:

- Newsletter changes
- Member Editorial
- ASIS International President's Message
- Council Member Profile/Spotlight

Inside this issue:

Upcoming ASIS Events	2
ASIS Professional Development Programs	2
Webinars	2
In the News	3
Cyber Security News	6
Member Editorial & Council Spotlight	9
ASIS President's Message	10

New Look for the Newsletter!

Spring/summer is upon us and the season of re-birth is the perfect time to introduce something new. As you may have already noticed, the ASIS Banking & Financial Services Council newsletter has been completely re-designed. The communications committee, has not only improved the visual appeal of the newsletter but has created a new vehicle to better inform you of all the quarterly news and activities occurring across ASIS and the council.

Previously, the newsletter was broadly oriented to upcoming programs and events. The new format will also encompass interesting news, member submissions, editorials, and other highlights. As an example, please refer to the back page article covering the first of many council member "spotlights". (And yes, those of you wondering, Hector forced the junior member of the committee to be the guinea pig!)

Of course, some things will largely remain the same, particularly the newsletter's emphasis on communicating information of interest to practitioners involved in Banking and Financial Services security, training and upcoming events.

As always, the newsletter is produced just for our members. We thank you warmly for your support and if you have any suggestions about content we would love to hear from you. Member submissions are always welcome!

Happy reading! – ASIS B&FC Communications Committee

ASIS BOARD CERTIFICATION 35th 1977-2012

35 Years of Board Certification!

ASIS INTERNATIONAL

Advancing Security Worldwide®

Security is always excessive until it's not enough.

- Robbie Sinclair

Upcoming ASIS Events

ASIS Board of Directors Election

Vote Online

Make sure you vote for the board of directors, online voting is open until August 3rd!

Go to:

www.asisonline.org

ASIS 2012

ASIS INTERNATIONAL

58TH ANNUAL SEMINAR AND EXHIBITS

September 10-13, 2012 | Philadelphia, PA

Don't forget to register soon for the Annual Seminar and Exhibits in Philadelphia.

Early indications are that hotels are filling up quickly!

ASIS Professional Development Programs

"Take the Challenge: Earn your CPP, PCI or PSP"

July 9th, Executive Protection—Dallas, TX

July 9th, Resilience Management Lead Auditor Certification—Alexandria, VA

July 11th, 2nd Annual CSO Roundtable Congress—Mexico City, Mexico

July 16th, Security Force Management—Boston, MA

July 16th, Physical and Logical Security: Advanced Applications and Economics—Boston, MA

July 18th, Investigative Interviewing Methods—Boston, MA

No Programs Scheduled for August

Annual Seminar in September

Register at:

www.asisonline.org

Webinars

July 11th, Open Source Intelligence: How to Use Open Source Information as Intelligence— Webinar

September 25th, Achieving ASIS Board Certification: The CPP Journey—Webinar

October 9th, Taking the Mystery Out of PSIM—Webinar

October 23rd, Achieving ASIS Board Certification: The CPP Journey—Webinar

Register for ASIS webinars at:
www.asisonline.org

Increased professionalism through development.

In the News

Create an Anti-Fraud Corps
Security Management (04/01/12) Vol. 56, No. 4, P. 58 Sherrod, Mike

With statistics from the Securities and Exchange Commission showing that fraud is a growing problem for U.S. businesses, it is becoming increasingly important for companies to have programs in place to respond to suspected cases of fraud. Such programs should make it clear who within the company is responsible for examining allegations of fraud and responding to them.

One way that companies can do this is by creating a fraud, risk, and investigations oversight committee that is made up of members of a number of departments, including security, human resources, and IT. The first issue that such a committee needs to address is the creation of a fraud oversight response plan for dealing with fraud. This plan should detail a process for preserving information that may be relevant to a fraud investigation. The plan should also make it easier to determine who should be involved with investigations into allegations of fraud.

The members who are included in the investigative team will vary based on the type of fraud that is being investigated. Once the initial information has been collected and the make up of the investigative team has been determined, the actual investigation can begin. Among the things that the company should do at this point is to prevent the fraud from continuing.

After the investigation has been completed, the company will present the findings to the relevant stakeholders, such as the board of directors, the audit committee, and external parties who need to be made aware of the situation. Companies need to carefully consider whether limits should be placed on the disclosure of sensitive information from the investigation.

Finally, companies should focus on how to deal with the vulnerabilities that allowed the fraud to occur in the first place. Following these steps is an important part of reducing the likelihood of fraud.

Major Breaches Could Undermine Consumer Confidence, Experts Warn
Bank Technology News (04/03/12) Fitzgerald, Kate

Major data breaches of payment card networks threaten to shake consumers' faith in issuers, despite the large strides the payment industry has made over the past several years to beef up security. "It's clear the fraud problem is not going away, and major breaches are not slowing up like we were sort of hoping," says Fiserv's Mike Urban. He also notes that many smaller breaches are occurring, with indications that these intrusions are escalating as well.

Some observers think each major breach upsets users' perceptions of the integrity of payment systems, which adversely affects adoption and use. "[The recent Global Payments] breach is not an isolated incident and will cement the idea in many consumers' minds that credit cards are, in some sense, untrustworthy," warns Voltage's Terence Spies. He also says the cost of reassuring customers and responding to potential losses stemming from a breach will be an administrative morass, while Urban says the broad publicity of the breaches tarnishes the reputation of financial institutions.

There also is the possibility that criminals may not immediately act on compromised card information, and instead hold it in reserve while waiting for the black market for such data to recover, notes McAfee's Brian Contos.

Phishing and malware meet check fraud
April 24, Help Net Security

Trusteer recently

Cyber Security—One of the most intense challenges of our time.

"Foreign Spies Stealing U.S. Economic Secrets in Cyber Space"

Develop a program to respond to allegations or suspicions of fraud in your company!

The FBI reports a rise in bank robberies reported in South Florida for 2012!

“Protect America’s Trade Secrets” - FBI

Rash of suspicious envelopes sent to New York City Banks!

In The News (cont.)

uncovered a scam in an underground forum that shows how data obtained through phishing and malware attacks can be used to make one of the oldest forms of fraud — check forging — even harder to prevent.

The scam involves a criminal selling pre-printed checks linked to corporate bank accounts in the United States, the United Kingdom, and China. The criminal is selling falsified bank checks made with specialized printing equipment, ink, and paper. For $5 each, they will supply checks that use stolen data provided by the buyer.

Russian cybercriminals earned $4.5 billion in 2011

April 24, IDG News

Russian-speaking hackers earned an estimated $4.5 billion globally using various online criminal tactics and are thus responsible for 36 percent of the estimated total of $12.5 billion earned by cybercriminals in 2011, Russian security analyst firm Group-IB said in a report published April 24. The researchers estimate the total share of the Russian cybercrime market alone doubled to $2.3 billion, while the whole Russian-speaking segment of the global cybercrime market almost doubled, to $4.5 billion.

FBI: South Florida bank robberies on rise

April 25, Associated Press – (Florida)

The FBI said bank robberies are on the rise in south Florida in fiscal year (FY) 2012 and may surpass the totals for each of the past 2 years, the Associated Press reported April 25. The FBI's Miami Field Office said there were 49 bank heists between October 1, 2011 and the end of March in Florida counties stretching from Martin to Monroe. Those numbers are up 25 percent compared with the same time frame in FY 2011.

Envelopes With White Powder Sent to Mayor and 6 Banks

New York Times (05/01/12) McGeehan, Patrick

Envelopes containing white powder were sent to New York City Mayor Michael R. Bloomberg and six banks in Manhattan, officials said Monday, ahead of planned May Day protests across the country. The powder, later found to be harmless, caused evacuations and shutdowns of the bank branches and a city building while the police and fire departments investigated. No one has claimed responsibility for the incidents.

FBI's New Campaign Targets Corporate Espionage

Wall Street Journal (05/10/12) Perez, Evan

The FBI on Friday launched a campaign to increase awareness about the threat from corporate espionage.

As part of that campaign, billboards have been put up in nine U.S. cities featuring the slogan "Protect America's Trade Secrets" as well as the address of an FBI Web site that includes tips on how to identify those who may be involved in the theft of sensitive corporate information.

The campaign comes as state-sponsored corporate espionage against U.S. companies is becoming a bigger and bigger concern. The corporate espionage cases that have been opened since the beginning of the current fiscal year have resulted in more than $13 billion in economic losses, a figure that includes the estimated future market value of trade secrets that have been stolen.

In addition, the federal government is increasingly seeing corporate espionage as a national security concern. FBI Assistant Director for Counterintelligence Frank Figliuzzi said that this is because jobs are lost when trade secrets are stolen, and that the loss of jobs during a difficult

In The News (cont.)

economic period represents a threat to the security of the nation. Meanwhile, foreign intelligence agencies are increasingly targeting companies that do not have sophisticated security measures in place to protect their trade secrets, such as the makers of software and other types of products.

Figliuzzi noted that foreign intelligence agencies are typically interested in products and research that have not yet made it to the market but could become components of new technology at some point in the future.

Ten Commandments for Effective Security Training

CSO Online (05/03/12)
Ferrara, Joe

Some organizations are not achieving the progress that they had hoped for in improving security awareness because their training programs consist of long lectures and slides that do not hold the attention of trainees. In addition, some organizations do not put much thought into what kinds of material should be taught in security awareness training programs, nor do they take the time to consider how the material should be presented. Organizations can avoid such pitfalls by observing a number of different principles when developing their security awareness training programs. For instance, organizations should keep training sessions short, since people learn more effectively when they can focus on a small amount of information instead of an overwhelming amount of new knowledge. In addition, trainees should be given an opportunity to learn by doing, such as exercises that allow them to practice identifying phishing attacks as well as those that help them practice how to create secure passwords. Although hands on learning is important, lectures are still a necessary component of any training program. Organizations should also keep in mind that training should not be a one-time event, since employees will learn if they receive frequent feedback and opportunities to practice what they learn. Finally, training programs should keep trainees engaged by using stories that contain characters and narrative development. Such stories are effective at holding the attention of trainees because they create subtle emotional ties to the material covered in the training session.

Prevent Workplace Fraud

CFO.com (05/16/12)
Johnson, Sarah

A recent study by the Association of Certified Fraud Examiners (ACFE) has found that workplace fraud that is committed by managers or executives can go undetected for as long as two years, though fraud perpetrated by lower-level employees usually goes unseen for only one year. Executives and others with higher levels of authority are usually able to hide fraud for longer periods of time because employees may be hesitant to report them, and because people in positions of authority are usually in a better position to override controls or conceal their misconduct, ACFE found. ACFE recommends that companies take steps to reduce the amount of time it takes to uncover cases of fraud or prevent it from happening altogether. For instance, ACFE recommends that companies require all employees to take vacations on a regular basis, since fraud is often detected when an employee is filling in for a colleague who is out of the office. Audits that are carried out without warning are also effective at reducing the amount of time that fraud is concealed, ACFE said. In addition, the organization noted that companies should perform employment verification, criminal and civil background checks, credit checks, and education verification on prospective employees. Finally, ACFE urged organizations to implement an open-door policy that allows employees to

Make your security training effective to achieve increased awareness across the organization!

> ***"Fraud committed by managers or executives can go undetected for as long as two years"***

Check out ACFE's recommendations for preventing workplace fraud!

In The News (cont.)

Operation Card Shop nets 24 arrests for credit card theft!

speak freely about pressures they are experiencing, as well as anonymous surveys that help them determine the level of workplace morale.

Tulsa Man Charged with 'Terrorism Hoax' for Threat to Bank
Tulsa World (06/22/12) Harper, David

A 53-year-old transient from Tulsa, Okla., was in court Friday on charges of making a "terrorism hoax" for threatening violence against a bank. Timothy Paul Kavanaugh was arrested the weekend before, after a Direct Express employee reported that Kavanaugh had threatened to take an AK-47 and carry out a shooting and bombing against an unspecified Comerica Bank branch. Comerica, which operates primarily in Texas, Arizona, California, Florida, and Michigan, does not operate any branches in Oklahoma. Direct Express offers Comerica prepaid debit cards to Social Security and Supplemental Security Income recipients who prefer to receive their benefits electronically.

FBI Says 24 Are Arrested in Credit Card Theft
New York Times (06/26/12) Schwartz, Nelson D.

Twenty-four people were arrested Tuesday in a crackdown on Internet credit card fraud after an extensive undercover operation in the United States and overseas. Two individuals were arrested in New York, nine elsewhere in the United States and 13 in a dozen other countries, according to a spokeswoman for the Federal Bureau of Investigation. In the sting, which was called Operation Card Shop, undercover investigators created an online bazaar to catch buyers and sellers of stolen credit card data and other private financial information. They also aimed at people who produce the physical credit cards that are then used to buy merchandise.

Cyberespionage: “Companies of all sizes could be targeted for the valuable information they may store or have access to”

Cyber Security News

The new generation of cold warfare!

Cyber Warfare: The Next Cold War
SC Magazine (04/02/12) Lawton, Stephen

Security experts say that countries around the world are now participating in a new generation of cold warfare via cyberattacks and defense. China and Russia are currently considered the leaders in this new battlefront, mounting a number of state-sponsored attacks against the United States. However, North Korea, Iran, France, Israel, and the United States itself all have rapidly expanding cyber warfare programs.

The U.S. government refused to name specific countries believed to be participating in cyberattacks until the National Counter Intelligence Executive released a report in late 2011 entitled “Foreign Spies Stealing U.S. Economic Secrets in Cyber Space." The report states that, “Certain allies and other countries that enjoy broad access to U.S. government agencies and the private economic sector conduct espionage to acquire sensitive U.S. information and technologies."

The report also cited four factors leading to the development of the cyberwar landscape in the next three to five years, including the further spread of mobile devices and

Cyber Security News (cont.)

smart phones; an economic shift that changes the way stakeholders share computing and networking resources; a cultural shift in the U.S. workforce that allows younger employees to mix personal and professional activities; and a geopolitical shift in the globalization for the supply chain that could increase access for foreign actors to compromise the integrity and security of computing devices.

Cyberattacks are also not limited to government targets, China, for example, is widely known to engage in a wide range of cyber espionage against civilian U.S. companies, particularly technology and security companies. Scott Crawford, research director for security and risk management at Enterprise Management Associates, with corporate headquarters in Boulder, Colo., agrees that companies of all sizes could be targeted for the valuable information they may store or have access to.

Many countries and companies will steal information with the goal of advancing their own ability to compete economically. Crawford encourages companies not to look for easy fixes to these risks, arguing that they should instead ensure they understand the complete profile of the risks they face.

How to Defend Against Infrastructure Attacks
Dark Reading (06/14/12) Higgins, Kelly Jackson

People take for granted the general underpinnings of the Internet, which was developed in friendlier times and was designed to be usable rather than secure, say Gartner's John Pescatore and Lawrence Orans.

The researchers cite four main attacks that exploit the aging Internet infrastructure and offer strategies for buffeting against them. Analysts say about half of all ISPs get hit with DDoS attacks each month, and the better attackers become at hiding what they are doing, the harder it is for security professionals to protect their organizations.

Meanwhile, many experts say new strategies are needed to combat the plethora of certificate authority-type breaches and attacks that have emerged, and Gartner says one way to mitigate this threat is with certificate management tools and hardened browsers.

Although attacks against the Internet's DNS root servers are relatively rare, analysts say organizations must take steps to ensure their DNS servers are protected because of the potentially devastating consequences. Most DNS attacks occur against older versions of software, and one barrier to these types of attacks is DNSSEC, which digitally signs domains to ensure their legitimacy.

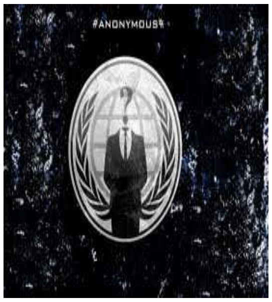
Finally, the transition from 3G technology to the faster 4G has opened organizations up to brand new vulnerabilities, with "mixed environments" being frequent attack targets.

Gartner suggests using a virtual private network or application-level security for any sensitive applications that operate on wireless devices for the next three years.

Cyber Security Threats, Infrastructure Sabotage Rising: McAfee
eWeek (06/19/12) Eddy, Nathan

A new cyber security report issued by McAfee and the Pacific Northwest National Laboratory (PNNL) examines the emerging cyber threats of the day and calls for a shift toward "security by design" in IT infrastructure.

The study points to ever-expanding networks with more access points and more automation creating new vulnerabilities as security is applied haphazardly and piecemeal.



Groups like Anonymous have generated highly visible attacks against very large organizations in the last several months.

"About one-half of all Internet Service Provider's get hit with DDoS attacks each month"

Cyber Security News (cont.)

"Cyber security must be embedded into the systems and networks at the very beginning of the design process"

The report also observes that cyberattacks have matured into a refined and carefully designed digital weapon for a specific purpose, and analyzes how emerging weaknesses of control systems continue to accelerate.

PNNL's Philip Craig Jr. says the "maze of disparate, multi-vendor, and stacked security tools" used to protect networks and IT infrastructure today can at best delay the determined cyberattacker and at worst make their job easier, offering up unforeseen weaknesses for more skilled assailants to exploit.

The report instead advocates security by design, a unified approach utilizing security features such as file integrity monitoring, hard disk read/write protection, and memory protection to create more secure systems. "Cyber security must be embedded into the systems and networks at the very beginning of the design process so that it becomes an integral part of the systems' functioning," says McAfee's Phyllis Scheck.

Budget Pressures, Workforce Woes, and Cyber Threats Converge

Federal Computer Week (VA) (06/27/12) Corrin, Amber

Although cyber security is the top concern of most federal CIOs, for more than 50 percent the lead priority is cutting costs, according to TechAmerica's 2012 Federal CIO Survey.

"Today, the number of things that CIOs need to do hasn't declined, yet they're being forced to find ways to innovate with less resources than they previously had," says George DelPrete with TechAmerica's CIO Survey Group.

Security officials at Immigration and Customs Enforcement, for example, cited delayed budget guidance and a depleted workforce market after the agency was criticized for awarding a sole-source IT security contract to their existing vendor rather than conducting bidding for the work.

Former Department of the Interior CIO W. Hord Tipton says a major element of the problem for federal IT is finding potential employees with the right skills to deal with the changing face of cyber security as a generation of experts ages into retirement. He says younger professionals are motivated by more than just high salaries, and suggests that federal IT consider offering benefits such as flexible work schedules and teleworking to attract top talent.

However, in the long term Tipton believes the existing pool of talent simply has to be broadened by encouraging and enabling the younger generation to pursue IT education.

Member Editorial—Dr. Hector Torres, PhD, CPP

After leaving the US Armed Forces and transitioning to the civilian sector, I was given some insights and advice on how to be a successful security practitioner in the 21st century by one of my closest mentors, Dr. Ralph Otero, CPP. Ralph highlighted that fact that the competency of professional security practitioners would be judged on three important criteria: years of experience in the security field, academic degrees obtained, and the professional certifications obtained. He further explained that while there is no substitute for experience acquired in field work, security practitioners desiring to climb the corporate ladder needed to pursue graduate studies and acquire professional certifications to set an individual apart from the rest of the security practitioners. Ralph continued to explain the role of ASIS and the importance of their certification program.

He expounded on the fact that once being professionally certified meant that you had to continually educate yourself to maintain the certification. In other words, as practitioner you would always be a student of security.

I followed my mentor's advice and took up the challenge of becoming a CPP. In 1999, I obtained my CPP certification and the certification is one of my most meaningful professional achievements. I now belong to a vast brotherhood of professional security practitioners who accepted the challenge and maintain the standards for others to follow. The CPP certification has truly set me apart professionally but most of all it has shown me that being a CPP is much more than having a three letter designation, it has become a fulfilling way of life.

"The only real security that a man can have in this world is a reserve of knowledge, experience and ability"

- Henry Ford

Council Spotlight

Roy Harness is the Director of Incident Management for Fiserv, Inc., the leading global provider of information management and electronic commerce systems for the financial services industry, driving innovation to generate best-in-class results for our clients. The Incident Management team manages incidents that threaten enterprise financial, legal, regulatory, and/or reputation interests for Fiserv. Prior to his current position, he served in the U.S. Army, was a law enforcement officer for almost 20 years and most recently managed the Physical Security & Safety group for Fiserv.

After transitioning from the public sector to the Physical Security & Safety group with Fiserv, the most important milestones set for acclimation to the role was membership in ASIS and attainment of board certification as a Certified Protection Professional. Roy's mentor and former ASIS Banking & Financial Services Council member, Bob Ballagh, preached and believed in the importance of board certification through ASIS for his team members as a tool to build a truly professional organization.

Raised in Columbus, Ohio Roy is married with four children, two of which will be starting college this fall. Roy obtained his Bachelor's Degree from The Ohio State University and his Master of Science in Public Administration from Central Michigan University.

BANKING & FINANCIAL SERVICES COUNCIL MEMBERS

CLARK CUMMINGS, CPP—CHAIR
FIRST BANK

RICH LAVA—VICE CHAIR
CITIBANK

BRIAN S. ISHIKAWA, CPP—SECRETARY
BANK OF HAWAII

CHARLES ANDREWS
FIRST DATA CORPORATION

STEVEN K. BRADEN, CPP
CAPITAL ONE FINANCIAL CORPORATION

LARRY BROWN
FIRST CITIZENS BANK & TRUST

STEPHANIE CLARKE, CFSSP
KEY BANK

ROBERT D. CROSKEY
WELLS FARGO & COMPANY

SCOTT DERBY
STATE STREET CORPORATION

ROBERT DUNLOP, CPP
TD BANK

ROY HARNESS, CPP
FISERV

ALEXANDER HILTON, CPP
CIBC

TERRY HUSKEY, CPP CFSSP
WELLS FARGO & COMPANY

DOUG JOHNSON
AMERICAN BANKERS ASSOCIATION

RICK MERCURI, CPP
RBS CITIZENS

MICHAEL NEUGEBAUER, CPP
FIFTH THIRD BANK

JAMES SMITH
BANK OF AMERICA

KEVIN SMITH, CPP
SALLIE MAE

HECTOR R. TORRES, PHD, CPP, CFE
BANCO POPULAR DE PUERTO RICO

ASIS President's Message

July 2012 Countdown to ASIS 2012

I hope by now you have set aside September 10-13 for the ASIS Annual Seminar and Exhibits. I attended my first show in 1991 and quickly determined that this event would find a permanent place in my annual professional development calendar. It offers by far the best ROI—both in time and money spent. Now, as president of ASIS, it's my privilege to welcome you to this year's event in Philadelphia. I hope you will stop by and say hello – whether at Sunday's First Time Attendee/New Member Reception or Monday's President's Reception at the National Constitution Center.

I recently put together a short list of tips to help assist first time attendees get the most from their time in Philadelphia. I'm sharing these suggestions here because whether it's your first time or fifteenth, I believe this advice can benefit all attendees.

1. **Pre-Network**. Thousands of security professionals from around the world will be at ASIS 2012. My guess is many are active in LinkedIn, Facebook, and Twitter. If you use these platforms, I encourage you to follow @ASIS_Intl (you can follow me @eduardemde) on Twitter and use the event hashtag #ASIS12 to post about Seminar, "like" our Facebook page, or join pre-Seminar Linkedin discussions to find and engage speakers, fellow attendees, and exhibitors.

2. **Do your prep work**. Know where your hotel is in relation to the convention center. Map it if you need to. Go early to get your badge and see how long it takes to get there. Add time to that for traffic and plan accordingly. Also, be sure to check the online show planner ahead of time and flag sessions you want to see. The Seminar website is worth checking out regularly for the session spotlights. In June there were two profiles – Physical Security Professional 2022 and Personal Mobile Devices in the Enterprise – as well as a post on all the Standards and Guidelines sessions. ASIS will soon launch its mobile app, which you can use to manage on the go. Use these tools to book appointments with exhibitors, plan which events you'll attend, and set your education schedule with backup sessions in case you find yourself in a session that isn't what you expected.

3. **Make a plan**. The show floor is 230,000 square feet. It's easily one of the most overwhelming experiences for ASIS newbies. There will be giveaways, there will be refreshments, there will be representatives pitching the latest tech wizardry. It's by far the best opportunity you will have all year to demo new products and services and get the answers to your specific security challenges. Comfortable shoes are essential, as is staying hydrated. Meeting rooms tend to get chilly so think about packing a light sweater. Depending on how much you try to fit in you likely won't be eating full meals at traditionally scheduled intervals. Plan appropriately.

For international travelers, take time now to check out the online ASIS Bookstore for publications and ASIS branded materials. From personal experience, I know you can save a lot of money by eliminating postage costs and buying things at the onsite bookstore. I always bring an extra bag to Seminar and it usually returns home filled with books, disks, and materials shared by exhibitors and fellow members.

4. **Be social**. As valuable as the sessions are, the networking and connections you make at the conference are every bit as important. Bring a ton of business cards. You will go through them. There are lots of parties and events to attend. Don't be a wallflower! Get out and have some fun. You'll make friends that will last a lifetime.

5. **Be prepared to learn**. The seminar is the largest congregation of security management professionals on the planet. The amount of knowledge you will glean in education sessions, hallway conversations, and networking breaks is tremendous. Absorb it, take notes. As you consider your education schedule, I encourage you to set time aside for the general sessions and keynotes. The general sessions offer a valuable opportunity to learn from some of our industry's most visionary leaders. The keynotes provide fresh insight and perspectives on global issues. Don't forget to pack your phone/tablet charger. Wi-Fi will be available in select locations around the convention center.

I hope these tips help you make the most of your time at Seminar. I look forward to seeing you in Philly!

Eduard J. Emde, CPP
President, ASIS International

Banking & Financial Services Council Advisory Members

Brian R. Abraham, CPP Bob Ballagh, CPP Robert Pearson Johan D. DuPlooy, CPP Douglas W. Kohldorf, CPP