ASIS Councils
NEWSLETTER

Banking and Financial *Services Council*

Clark Cummings, CPP – Chair
FirstBank

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 Corp

Larry Brown
First Citizen Bank & Trust

Stephanie Clarke, CFSSP
Key Bank

Robert D. Croskery
Wells Fargo & Company

Scott Derby
State Street Corp

Robert Dunlop, CPP
TD Bank

Roy Harness, CPP
Fiser

Alexander Hilton, CPP
CIBC

Terry Huskey, CPP, CFSSP
Wells Fargo

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

Advisory Members

Brian R. Abraham, CPP
3SI Security Systems

Bob Ballagh, CPP
Ballagh Consulting

Johan D. Du Plooy, CPP
Risk Diversion Pty Ltd

Douglas W. Kohldorf, CPP
Tri Tower Group, LLC

Robert Pearson
Lear Security Group

Banking and Financial Services Council
January – March 2012

Greetings to all Banking and Financial Security Professionals!!

The Banking and Financial Services Council has started 2012 running with a full year agenda. Our new Chair, Mr. Clark Cummings along with Rich lava, Vice Chair and Brian Ishikawa, Secretary are leading the Council's efforts. As part of its agenda, our Council is planning to sponsor a Pre Conference Workshop at this year's annual conference on Sunday, September 9th in Philadelphia, PA, This year Pre-Seminar Workshop promises to be a spectacular one. If you attended last year's you will not be disappointed with this year's workshop. Additionally, the Council plans to be involved in multiple activities to strengthen our members' professional development. We envision a great year full of professional challenges and successes.

Board of Director Nominations

ASIS International has notified its First Call for petitions for nomination of candidates for election to the Board of Directors. Your attention is invited to Policy and Procedure Guides 1021, for guidance concerning eligibility criteria, petition and voting procedures. Effective January, 1997, Section III A states: "At the time of nomination, a candidate must be either, 1) an individual who is primarily responsible for the professional application of security principles and practices in the private or public sector in a position of responsible charge; and/or 2) a Certified Protection Professional (CPP) in good standing; and/or 3) a full-time educator or training professional who provides instruction in security, conducts security research or administers a security or crime prevention program at an accredited educational institution or at a professionally recognized training institute". As a reminder, the entire election process will be conducted on line, beginning March 7, 2012.

Upcoming Events

ASIS
NYC
22ND NEW YORK CITY
SECURITY CONFERENCE & EXPO
APRIL 25-26, 2012 | NEW YORK, NY
JACOB JAVITS CONVENTION CENTER

ASIS Professional Development Programs

Apr 15-17: **11th European Security Conference & Exhibition**

Apr 16-17: **Enhanced Violence Assessment and Management**

Apr 18-19: **Active Shooter**

Apr 27-28: **Classroom Review - CPP | PSP**

May 7-10: **Crisis Management: Introduction to the Response Plan and Advanced Topics**

May 7-10: **ASIS Assets Protection Course: Practical Applications (APC II)**

May 7-12: **Resilience Management Lead Auditor Certification**

May 17-18: **Certification Reviews - CPP | PSP**

May 21-24: **Managing Your Physical Security Program**

Webinars

Apr 3: Cyber Security: Defining the Threat

Apr 18: Ten Years Since 9/11: 1,389 Years of Islam...What Has Changed in a Decade?

Apr 25: Incident Command System (ICS) and Interfacing with Agencies that Utilize It

May 16: Lessons Learned: Trends in Extreme Violence in the Workplace

May 23: Safeguarding Intangible Drivers of Company Value

IN THE NEWS

Diebold Virtualizes ATMs To Secure Banking Data
01/04/2012, InformationWeek

Automatic teller machine maker Diebold has taken a novel approach to protecting bank customer data: virtualization. Virtualized ATMs store all customer data on central servers, rather than the ATM itself, making it difficult for criminals to steal data from the machines. Diebold last year partnered with VMware to produce a zero-client ATM. An inaccessible zero-client component causes the ATM screen to render the results of interactions with a virtual machine running on a central server in a bank or Diebold data center. No customer data is captured and stored on the ATM itself, and all data storage devices have been removed. Westfield Bank, Palmetto Bank, and BellCo Credit Union are among the U.S. institutions that use Diebold ATMs, ATM management, or ATM security services.

Feds Bust $1.5 Million ATM Skimming Scheme
01/10/2012, InformationWeek

Federal officials have announced the arrest of a Romanian citizen who allegedly installed card skimmers on more than 40 ATMs in the New York City metropolitan area. Prosecutors have accused the suspect of participating in a fraud ring that netted at least $1.5 million via the card skimmers between May 2011 and January 5, 2012.

Core Security Values: Do You Have Them?
01/12/2012, Security Magazine

For those involved in the practical, day-to-day operations of security departments, the value statement works as a method of marketing the department's work and has the added benefit of guiding decision making. A value statement is an expression of core beliefs; "customer service is job one," for example. Most customers who rely on security services want convenience, simplicity, and virtually invisible -- as in, inconspicuous -- access to where they want to go. Most users have no interest in the ins-and-outs of access and ID and likely little concern for security's operational challenges to delivering these services, so keep it separate from values. Here are a few examples of where to begin some fundamental values statements. In access control, it is the responsibility of the security access control department to provide the most convenient form of access to employee areas. In ID checkpoints, it is the security department's responsibility to usher employees and visitors through ID checkpoints in a fast and friendly manner. Values statements such as these can be both simple and obvious, and can easily be based on principles of convenience, courtesy, and prompt service. While delivering these services is another matter, the statements are a great place to start. A security executive can begin by gathering staff together for an informal meeting about access controls. Write the mission statement on the board -- "to provide a safe and secure environment for our business," for example -- and proceed to brainstorm concepts such as delivering the most convenient form of access, quick and friendly access points, and so forth, and see where it goes. Remember to start with a general discussion and save concerns about operational needs for later.

PIN Authentication Versus Signature Authentication
01/23/2012, Portals and Rails

Financial institutions' risks from various payment types can be assessed by comparing fraud losses on a per-unit basis, and doing this for credit card, signature debit, and PIN debit transactions illustrates PIN authentication's effectiveness for preventing payment card fraud, writes the Atlanta Fed's Douglas A. King. He cites Nilson Report's findings that on a per-transaction basis, yearly credit card-related fraud losses peaked in 2010 at 7.5 cents a transaction—a nearly 9 percent increase from 2006. On a dollar-volume basis, credit card fraud losses climbed by almost 27 percent during this same period, to 8.5 basis points in 2010 from 6.7 basis points in 2006. Although a PULSE Debit Issuer Study pointed to a steady increase in debit card fraud losses as well, King notes that signature debit transactions comprised an estimated 91 percent of total debit card fraud in 2010. "Based on per-unit fraud losses of credit and debit cards, financial institutions have significantly more exposure to fraud losses from card payments with signature authentication than from those with PIN authentication," he says. "Yet PIN authentication is not accepted for credit transactions, and it accounted for only 32 percent of debit card purchase transactions in 2010." King attributes the large difference between per-transaction fraud losses between credit card and signature debit transactions to credit card transactions having an average ticket size of about 2.5 times that of signature debit transactions. "Ultimately, PIN debit offers an additional and superior layer of authentication not offered on credit and signature debit transactions," he concludes.

Adding Weapons to ATM Defenses
01/26/2012, Wall Street Journal

ATMs have become big targets for thieves. According to the FBI, more money is stolen by thieves who compromise ATM systems and perpetrate other types of data breaches than by thieves who rob bank branches. Robbing an ATM can be lucrative, as a typical ATM heist nets thieves 10 times as much cash as a bank robbery, the American Bankers Association says. Faced with these threats, ATM manufacturers are taking steps to improve the security of their machines. Diebold, for instance, is developing an ATM that uses cloud computing to store information in a remote location instead of in the ATM itself. Diebold says that the use of cloud computing would make ATM software easier to protect, as it would be stored in a centralized location. However, some security experts believe that putting large amounts of data in the cloud will make cloud computing systems a target for hackers. Meanwhile, the Brazilian company Itautec is wrapping up development on a prototype ATM that uses holographs that consumers use to make transactions with hand gestures. Consumers will not be able to touch the ATM itself, except for the part that dispenses cash, as most of the machine will be protected by bulletproof glass. Other ideas that are in the works at other companies are ATMs that require consumers to tap their phones instead of swiping their cards in order to make transactions. Such technology is designed to cut down on skimming. Despite the security threats to ATMs, it is unclear whether banks will invest in these technologies, given the fact that many financial institutions are under a great deal of pressure to reduce their costs.

Why Skimming Won't Go Away
01/27/2012, BankInfoSecurity.com

Card skimming attacks remain a potent practice whose use has not subsided, despite expanding initiatives to spread awareness of skimming fraud, because skimmers continually shift their targets to areas where people are less informed. Evidence of this trend has surfaced with an advisory on skimming at local ATMs and pay-at-the-pump gas terminals issued by police in Wendover, Nevada. "It's not uncommon for small communities to inherit the problems of larger cities nearby, as fraudsters migrate their scams to areas where consumers are less aware of the possibility of having their payment cards skimmed," says FICO's' John Buzzard. Zions Bank's Chuck Groat reports that pay-at-the-pump skimming attacks remain simple to execute, and he says that merchants currently lack suitable incentives or penalties to reduce such attacks. Convenience stores and gas station owners have been daunted by the expense of gas terminal security upgrades, but consultant Robert Siciliano says these merchants "don't stand a chance in fighting this crime unless they collectively make significant changes and upgrades in the security of their existing technologies." To encourage merchants to upgrade their equipment, MasterCard and Visa have announced mandates for EMV card technology upgrades by 2013 and 2015, with liability for fraud losses falling on the shoulders of non-compliant retailers. "If the compromised entities, to include ATM owners, shared in at least some of the overall loss exposure that their skimmed self-service terminals caused, then you would see more investment to prevent these types of activities," Groat says.

MasterCard Joins Push on New Card Technology
01/30/2012, Wall Street Journal

MasterCard and Visa have joined forces to push merchants to upgrade to new checkout systems that accept credit and debit cards that store information on a computer chip rather than a magnetic stripe. These chip-enabled cards, which are common internationally, are designed to cut down on fraud. Merchants have been hesitant to make the conversion as long as the benefits and requirements of doing so differ across card companies, which has led to the partnership between MasterCard and Visa. Both companies also say they will require banks that handle their cards to use chip-based systems by April 2013. To provide an extra incentive to merchants, they have additionally agreed to hold businesses accountable for any fraud that occurs if they have not yet upgraded, while promising they will reduce security assessments for those that do agree to make the switch beginning in October 2013.

Unlike Visa, Merchants Pushing PIN for Chip Cards in U.S.
01/31/2012, American Banker

Merchants are urging the establishment of chip-and-PIN authentication for any U.S. effort for accepting chip cards supported by the EMV security standard, rather than the chip-and-signature option backed by Visa. Merchant Advisory Group CEO Mark Horwedel says that although merchants are keen to switch from magnetic stripe card acceptance to smart cards, they do not want to feel coerced into other payment technologies if they feel it lacks economic feasibility. He says retailers think that signature devices have a tendency to wear out and require replacement, while checkout lines are slowed down by shoppers writing signatures. Also frustrating for merchants accepting signature cards is the need to retain receipts in case of chargeback claims, which could entail sifting through many paper receipts in certain instances. Horwedel says retailers generally prefer chip-and-PIN because they are loath to make a heavy investment in point of sale upgrades without the return on investment of the security delivered by PIN. The Merchant Advisory Group is in favor of placing liability in fraud cases on whichever party does not adopt chip-and-PIN's fraud prevention measures, and it also backs technology advancing the use of chip-and-PIN for Web transactions.

A Pickup in Stickups Puzzles Police
02/03/2012, Wall Street Journal

In January, 40 bank holdups were reported in Southern California, mostly in Los Angeles and Orange counties, the FBI announced Wednesday. In 2011, there were 677 bank robberies in California, the state with the highest number in the nation, according to federal data. New York and Texas followed, with 339 and 274, respectively. Nationwide, robberies are down 30 percent since 2005 and fell 34 percent in California in the same period. In the past, banks were typically hit by teams of armed men who held customers and employees hostage during a heist, police said. Now, banks are more likely to be robbed by a single person who quietly slips in, threatens the teller and leaves with cash. Robbers typically get away with about $1,000. Shootings and serious injuries during robberies have been rare in recent years.

Jury Convicts 2 in $50M Bank Fraud Conspiracy
02/28/2012, Associated Press

Two people have been convicted by a federal jury for their roles in a $50 million conspiracy to commit bank fraud that authorities say relied on identity theft by employees of some of the largest U.S. banks. Julian Okeayaninneh and Olugbenga Temidago Adeniran were found guilty of multiple counts, and thus far 27 individuals have either pleaded guilty or been convicted in the scheme, which involved bank employees stealing customer identities, then buying and selling them so they could be used to create bogus accounts, apply for loans, and get cash. Victims included American Express, Associated Bank, Bank of America, Capital One, Guaranty Bank, JP Morgan Chase Bank, TCF Bank, U.S. Bank, Wachovia Bank, Washington Mutual, and Wells Fargo.

CYBER SECURITY NEWS

BITS: Tackling Fraud in 2012
01/06/2012, BankInfoSecurity.com

John Carlson, BITS' new VP of cybersecurity and fraud prevention, sees the evolution of technology introducing new threats to financial institutions and says banks can mitigate those risks by bringing key thought-leaders together. Another area is in the development of best practices and strategies for how to solve cybersecurity and fraud issues. BITS is focused on improving the identity-proofing process, or "know your customer." Carlson says BITS will continue working with the government and other parties to determine ways to improve KYC, "particularly in situations where you may never actually meet your customer face-to-face." BITS has combined the cybersecurity

and fraud program under Carlson's leadership, taking two very strong programs and finding ways to collaborate where there is an intersection between security, cybersecurity issues and fraud. To address risks, BITS will employ a combination of developing the best practices papers for its member companies to address issues in the fraud space, from mortgage fraud to remote deposit capture, to looking at social media and how it is being used, and new ways to perpetrate fraud. According to Carlson, regulators currently have a tremendous amount of authority and have issued a great deal of guidance and regulations in the cybersecurity, supplier risk, identity theft and fraud areas. They have a very strong foundation with existing rules and supervisory guidance. Carlson predicts a broader effort throughout the government working with BITS and financial institutions and others in the private sector to enhance information sharing, to develop some common standards around breach notification and other areas including research and development and other proposals that are currently being debated in the U.S. Congress. With regard to cybersecurity and fraud prevention in 2012, Carlson expects to help financial institutions in several ways: providing many forums for discussion that bring key people together to help solve the different problems, developing best practices and strategies for how to solve issues, and targeting particular industries where partnership and collaboration are needed to solve problems. Carlson says financial institutions are missing the mark on fraud prevention because of the challenging dynamic of trying to follow the market, meeting customer needs, customer demands, and strong controls that follow all of these. Vulnerabilities remain in areas such as mortgage fraud and ACH-type fraud, as well as how mobile devices are being used and how social media is being used.

Security Best Practices Reduce Downtime From Cyber-Attacks: Survey
01/24/2012, eWeek

Though there is no security panacea to prevent all attacks, Symantec's most recent survey shows that following best practices is a smarter defense than cutting corners on the protections. Organizations that invested in tighter defenses and trained employees to be more self-aware were in a stronger position to thwart or withstand attacks, Symantec found in its Endpoint Protection Best Practices survey. The top tier organizations in the survey were 2.5 times less likely to encounter a major cyber attack, and 3.5 times less likely to experience downtime compared to other organizations, according to Symantec's Jason Nadeau. Researchers wrote in their report that antivirus software is no longer effective by itself, and that the organizations that had used more sophisticated security technologies and practices were more ready and better able to circumvent attacks. Organizations with higher scores reported using various layers to guard their assets, including data loss prevention, intrusion prevention and detection systems, anti-malware, and firewalls. Almost all of the organizations in this group reported carrying out awareness training for employees. The policies and practices of respondents in the top tier contrasted "sharply" to those who ranked in the bottom tier, Symantec researchers wrote. The bottom tier organizations did not educate employees on security best practices that frequently. These organizations were more likely to experience steep losses following a successful cyber attack, the report found. Regardless of their ranking on the list, organization were not immune to cyber attacks and still experienced downtime and losses when safeguards failed.

With New Bank-Security Guidance, How Safe From Cybercrime Is Your Firm?
02/14/2012, CFO World

In June 2011, the Federal Financial Institutions Examination Council (FFIEC) issued a report designed to raise the safety of the funds held in corporate bank accounts. The guidance suggests that security at the perimeter of a network is no longer sufficient. Today's solutions need to improve the code within the applications themselves, and financial institutions should implement layered security programs, according to the report. This involves "the use of different controls at different points in a transaction process so that a weakness in one control is generally compensated for by the strength of a different control," the report said. Program components could include fraud detection, monitoring systems, and dual customer authorization via multiple devices, the guidance says. The solutions should additionally address processes that detect and respond to anomalous or suspicious behavior, account to the FFIEC report. Such systems must gather data on individual online banking sessions, including the computer, operating system, and network used, the customer's pattern of clicks, and the time and day at which transactions usually take place. With this information, the system is better able to spot unusual activity. Hunt Imaging LLC Chief Financial Officer Mike Stanek adds an extra layer of security by using a key fob registered to the company's bank account that regenerates a new number every few seconds.

FROM OUR ASIS INTERNATIONAL PRESIDENT

Eduard J. Emde, CPP
President, ASIS International

Celebrating Thirty-five Years of Excellence

As part of my travels this past month, I visited the France chapter and attended the 3rd Middle East Security Conference & Exhibition in Dubai. It was striking how often the subject of certification came up-individuals asking about the specifics of the programs and chapter leaders setting goals for themselves and their members. It seems the value of certification is often demonstrated by those who have been successful at attaining one or more credentials. Enthusiasm, commitment, and success breed more enthusiasm and success. Therefore, I challenge security practitioners who are certified to not hold back and to spread the word about their own path to certification. I especially encourage the ASIS volunteer leaders to lead by example and to guide members towards the board certification that best suits their professional needs.

Now in its 35th year, the ASIS certification program has a long and storied history. Launched at the 23rd Annual Seminar and Exhibits in 1977, the Certified Protection Professional (CPP) credential is recognized worldwide as an objective measure of an individual's experience and competency. It's why in 1998, I made the decision to sit for and earn my CPP. I wanted to validate the skills I had developed in security management.

Many dedicated ASIS leaders had a hand in creating the certifications. Former ASIS President Dick J. Cross, CPP, first proposed the idea to the Board of Directors in 1972. He believed if the security practice was ever going to become a security *profession*, then meaningful certification credentials were necessary. It took several years to finalize the criteria but in 1977, certification by review began, and the first CPP was awarded that year to ASIS president Wayne Hall. Over time it became clear that there was a need for specialty certifications and in 2003, the Professional Certified Investigator (PCI) and Physical Security Professional (PSP) were established. Later that year, James S. Cawood, CPP, PCI, PSP, became the first member to earn all three designations and I'm pleased to report that in 2011, Kristiina Mellin, CPP, PCI, PSP, from the Sweden chapter, became the first female "trifecta" practitioner. Today, there are 383 dual-certified security professionals and 61 hold all three ASIS designations. I applaud these practitioners for dedicating the time and resources to earn their credentials and through their daily work, raise the visibility and value of ASIS certifications. I would be remiss to not point out that for more than three decades, the members of the Professional Certification Board have proven to be good custodians as

well as future oriented leaders, and I offer my deepest thanks for all they have accomplished.

There are many reasons to earn a board certification. Studying for the exam alone will raise your understanding of the breadth of our profession and demonstrates a commitment to continuous learning. Joining or forming a review group is a terrific way to expand your professional network. You will connect with peers that have made the same commitment and can offer some much needed support along the way. The ASIS Linkedin group and CPP Certification Study subgroups offer excellent sounding boards for practitioners when there are no local review programs available.

Professional advancement is a top reason for many practitioners to earn their credentials. Year after year, the ASIS salary survey confirms that board-certified practitioners earn more than their non-certified peers. And, for those that are transitioning from the law enforcement or the military, an ASIS certification not only aids in that transition, but provides a solid foundation on which to build a private security career.

We plan to mark this 35th anniversary by spotlighting many of our certified members in the months ahead, including podcasts and a timeline of significant accomplishments. All these efforts will culminate with a special ceremony at ASIS 2012 in Philadelphia. Stay tuned to *www.asisonline.org* for details.

In closing, I hope if you meet the criteria to earn your CPP, PSP, or PCI that you take this opportunity to make the commitment now. I guarantee you will be challenged but your reward will be far greater than just the three letters after your name. By earning your board certification, you join a special group of practitioners who have demonstrated their commitment to professional excellence and to advancing the security profession worldwide.