

ASIS Councils NEWSLETTER

Banking and Financial Services Council

Terry Huskey, CPP, CFSSP – Chair
Wells Fargo

Clark Cummings, CPP – Vice Chair
FirstBank

Rich Lava -Secretary
Citibank

Charles Andrews
First Data Corporation

Brian R. Abraham, CPP
3SI Security Systems

Robert S. Ballagh Jr, CPP
BCS Security Consulting

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

Johan D. Du Plooy, CPP
Risk Diversion Pty Ltd

Roy Harness, CPP
Fiser

Alexander Hilton, CPP
CIBC

Brian S. Ishikawa, CPP, CFSSP
Bank of Hawaii

Doug Johnson
American Bankers Association

Douglas W. Kohldorf, CPP
Tri Tower Group, LLC

Rick Mercuri, CPP
RBS Citizens

Michael Neugebauer, CPP
Fifth Third Bank

Robert Pearson
Lear Security Group

James Smith
Bank of America

Kevin Smith, CPP
Sallie Mae

Hector R. Torres, PhD, CPP, CFE
Banco Popular de Puerto Rico

Banking and Financial Services Council

October – December 2011



Happy Holidays!!

It that wonderful time of the year again!! As we close out another exciting challenging , and yes, a somewhat trying year in the banking and financial sector, we need to reflect on all the challenges we have met, all the lessons we have learned, and on all the blessings we have received. While the economic front still poses a certain level of uncertainty, it is through hope, perseverance, teamwork, and vision that we can overcome the obstacles. Let us continue to work together to face the new challenges of 2012 and may these challenges help us to grow and prosper. On behalf of our outgoing chair, Mr. Terry Huskey and our incoming Chair, Mr. Clark Cummings, we want to wish you Happy Holidays and our best wishes for a Prosperous New Year!!

BFSC Council Changes

Our council will begin 2012 with a new Council Chair and Vice Chair. Mr. Clark Cummings and Mr. Richard Lava have been designated as our new Council Chair and Vice Chair respectively. We wish them continued success in their new responsibilities. We also want to thank Mr. Terry Huskey, our outgoing Chair, for his leadership, professionalism, and dedication as the Council's Chair during 2011.





ASIS Professional Development Programs

Jan 23-27: Wharton/ASIS Program for Security Executives (Week 2 of 2)

Jan 23-27: RABQSA-RES Resilience Lead Auditor Certification Course

Feb 3-4: Classroom Review - CPP | PSP

Feb 19-21: 3rd Middle East Security Conference & Exhibition

Feb 27-28: Conducting Corporate Investigations

Feb 27-Mar 1: Physical Security: Introductory Applications & Technology

Feb 29-Mar 2: Organizational Resilience

Webinars

Dec 14: Active Shooters in Healthcare Environments: Protecting Patients, Staff, and Visitors

Jan 19: Dynamic Communication for Career Success

Feb 15: Advanced Internet/Social Network Investigations and Background Checks

Feb 16: Cloud Computing and Software-as-a-Service: An Overview for Security Professionals

IN THE NEWS

5 Secrets to Building a Great Security Team 09/18/11, CIO

Tim Williams is a former head of ASIS International and currently serves as global security director for Caterpillar. He says it is essential to curb risks by first evaluating how the security team operates in order to identify issues that need to be addressed. He says enterprise security risk management (ESRM) involves taking a holistic view of the vulnerabilities faced by people, networks, and intellectual property. To this end, it is essential to define the team's processes clearly "in a well-written strategy or operating plan" to identify "issues that actually pose the greatest risk or threat to the enterprise." At Caterpillar, Williams also set up global crisis management processes and appointed personnel to formalize underserved functions the were to be monitored by newly appointed regional security directors. Williams also recommended that security team members get an MBA to ensure they can successfully support the organization and better understand corporate decision-making. Another important component in Williams' ESRM plan is naming a communications czar who helps ensure that staff realize the role they play in security, which can be implemented through newsletters and other publications. Furthermore, Williams wants his staff to conduct open talks on any subject even if they differ with management's views.





ID Theft Ring Arrests Reinforce the Importance of Bank Security

10/10/11, Bank Systems & Technology

News from the New York City borough of Queens that 111 individuals have been indicted in what is being called the largest identity theft takedown in U.S. history reinforces the importance of bank security. The defendants are allegedly members of five separate organized forgery and identity theft rings based in Queens and have ties to Europe, Asia, Africa, and the Middle East. They were charged in ten indictments with stealing the personal credit information of thousands of American and European consumers and costing individuals, financial institutions and retail businesses more than \$13 million in losses over a 16-month period. According to the DA's office, credit card account numbers were stolen by staff at banks, mostly by bank tellers, as well as restaurants and shops using skimming devices. According to the indictments, the stolen account numbers were ultimately sent to a "manufacturer" who re-encoded the information onto the magnetic strips of blank credit cards using a "reverse" skimming device. Bank executives are already concerned about security these days, with recent studies forecasting that bank losses due to cybercrime will increase steadily over the next several years.

Eleven Areas for Improvement

10/11/11, Security

Over six years of working with top-tier security leaders to develop research and solve problems, the Security Executive Council has found that Tier 1 Security Leaders are most often concerned with the lack of strategic vision and planning skills in deputies and other potential leaders they are grooming. Here are 11 key strategic areas in which Tier 1 Security Leaders would like to see initiative from their direct reports. The next generation of leaders must know how to align their programs with the risk categories most important to the Board. Security leaders who want to demonstrate their business-based contribution to the organization must know how to analyze metrics to identify risk, and use that data to tell a compelling story of organizational performance and value. Leaders need to be familiar with the latest global requirements for preparedness compliance, and they must take steps to establish community partnerships to help build resilience and protect their reputation. Up-and-coming security leaders must know how to roadmap protection architecture and how to manage information crises at the speed of the Internet. Security leaders must show security's revenue influence and cost avoidance in return-on-investment calculations and operating statement results. Leaders need to learn the steps to evaluate themselves and their organizations against industry research to inform their role and corporate preparedness. Security leaders must question how they can play a stronger role in an organization's ethical performance. Faced with epidemic-level fraud and identity theft, tomorrow's security leaders must be knowledgeable about multi-factor authentication of persons, cargo, conveyances, and information. Security leaders need to understand how to identify, develop, and retain talent at all levels for sustainable results. Security leaders need to know how to build and sustain partnerships with clients, governmental agencies, peer organizations, and trade associations. And finally, tomorrow's security leaders should know how to apply proven practices and innovative solutions to optimize core organizational processes and outcomes.

Bank Scams on the Rise

11/06/11, Wall Street Journal

According to the American Bankers Association, banking scams are on the rise. The industry group said the trend is expected to last through the holiday season, as consumers make more card purchases and often lose track of their spending. Many of these scams will be phishing attacks, in which an individual calls a consumer and claims to work for his bank. The scammer often asks for identifying information or claims he needs to verify a transaction. Once the fraudster has the information, it is relatively easy for him to access money in an individual's bank account or to open a





new line of credit. If consumers receive such a phone call or e-mail, they should hang up and call their financial institution directly to check if the call is legitimate or not.

When Financial Fraud Meets Facial Recognition, the Jig May Be Up, 11/18/11, Reuters

Facial recognition technology is starting to be more widely used in the banking industry as a fraud detection tool. Chip McBreen, who leads fraud prevention and security at Members 1st Credit Union in Pennsylvania, has become a believer in the technology. He says it has already delivered results for his institution many times. "We had a case last week where we had a person come in with a fictitious drivers license, and we actually used it (the technology) to determine that wasn't the member. ... It allows me to search for it (the image) very quickly and produce that for law enforcement."

94 Indicted in Scheme Exploiting a Bank 12/07/11, New York Times

An electronic crime was recently prosecuted in New York and led to the indictments of 94 individuals for stealing at least \$450,000 from TD Bank, and possibly as much as \$1 million. The suspects exploited a loophole in TD Bank's system that allowed new account holders to transfer money deposited into savings accounts to a checking account without a waiting period for the deposited checks to clear. Once the money was transferred, the participants quickly withdrew the money as cash at Western Union branches and casinos.

CYBER SECURITY NEWS

Most Enterprises Face Increased Malware Risk From Social Media 10/06/11, DarkReading

Enterprises are allowing workers to log into social networks from the office, but that privilege might be costing them, according to a new Ponemon Institute study published in early October. The study evaluated the social media readiness and risk profile of more than 4,000 IT and IT security practitioners across the world. Most respondents agreed that use of social media in the office is part of achieving business objectives, but they also believed that these tools exposed their organizations to risk. According to the study findings, these fears could be justified. Malware attacks have increased because of social-media usage, the study finds. Fifty-two percent of respondent organizations said they have witnessed an uptick in malware attacks as a result of employees' use of social media. This spike in social media attacks is catching many companies unawares, according to Ponemon. Just 29 percent of respondents said their organizations have robust social-media security controls. Diminished productivity was cited by 89 percent of respondents as the top negative consequence of a boost in social media, while 77 percent cited reduced IT bandwidth.

Georgia Tech Releases Cyber Threats Forecast for 2012 10/11/11, Georgia Tech News

A report from researchers at the Georgia Tech Information Security Center (GTISC) and the Georgia Tech Research Institute (GTRI) warned that 2012 will feature new and increasingly sophisticated means to capture and exploit user data, as well as escalating battles over the control of online information that threatens to compromise content and erode public trust and privacy. The report cited search positioning, mobile Web-based attacks and stolen cyberdata as areas of concern in the coming year. "If we are going to prevent motivated adversaries from attacking our systems, stealing our data, and harming our critical infrastructure, the broader community of security researchers--





including academia, the private sector, and government--must work together to understand emerging threats and to develop proactive security solutions to safeguard the Internet and physical infrastructure that relies on it," says GTISC director Mustaque Ahamad. "Our best defense on the growing cyber warfront is found in cooperative education and awareness, best-of-breed tools, and robust policy developed collaboratively by industry, academia, and government," says GTRI's Bo Rotoloni.

Wall Street Banks Get NSA Intel on Foreign Hackers **10/26/11, USA Today**

Due to heightened concerns over financial sabotage, the National Security Agency is sharing information on foreign hackers with Wall Street investment banks. As part of that effort, the NSA will share crucial information about malicious software. Additionally, the agency is considering expanding its pilot program that shares similar information with the defense sector. However, NSA director Gen. Keith Alexander failed to provide further details on the matter. The Federal Bureau of Investigation has previously warned financial institutions of specific and credible threats. The information sharing has been spurred by recent, sophisticated and coordinated attacks that pose a significant threat to the industry.

Five Million New Pieces of Malware Found in Q3 2011 **11/03/11, V3.co.uk**

Records plummeted again in cyberspace between July and September 2011 after 5 million new samples of malware were discovered, according to Panda Security. The firm's most recent quarterly PandaLabs report found a record number of Trojans, identifying roughly 75 percent of all samples as this kind of information-stealing malware. The number increased to over 76 percent from 68 percent between April and June, driven by cybercrooks trying to monetize malware attacks by stealing banking or other account log-in information. The second most ubiquitous type of malware was viruses at 12 percent, down more than 4 percentage points between the second and third quarters, while third place went to worms, dropping to 6.26 percent from 11.69 percent. Fake antivirus continues to be a nuisance, pushing the number of newly discovered adware samples up from 1.37 percent in the second quarter to 3.52 percent in the third. China was once again the nation with the most infections, followed by Taiwan and Turkey, according to Panda.

Teaming Up to Take Down Threats **11/10/11, Dark Reading**

A Federal Bureau of Investigation initiative called Operation Ghost Click used massive public-private cooperation to uncover a global click fraud scheme. The scheme infected more than 4 million computers and generated more than \$14 million for a criminal group comprising at least seven Estonian and Russian citizens. The group operated under various corporate names and allegedly infected victims' computers with malware that altered the systems' domain name servers and redirected requests for Web site addresses via hijacked hosts. The group is believed to have used the malware and servers for four years to create false advertising clicks to businesses that paid affiliate fees, thereby defrauding the firms. The FBI worked with the Estonian Police and Border Guard, the Dutch National Police, and NASA's Office of the Inspector General, while private-sector participants included Georgia Tech University, the Internet Systems Consortium, security firm Mandiant, anti-spam group Spamhaus, security intelligence firm Team Cymru, antivirus company Trend Micro, the University of Alabama at Birmingham, and members of an ad hoc group called the DNS Changer Working Group. McAfee's Phyllis Schneck said that public-private cooperation is crucial to investigating and prosecuting the criminals and agents behind online crime and intellectual property attacks. "This is what happens when the good guys make it work," Schneck said. "This is what happens when several companies can get together with nonprofits and work together with law enforcement to go across corporate boundaries and across international boundaries."





A Reason to Revisit Your Cybersecurity Risk **11/11/11, CFO**

Last month the Securities and Exchange Commission (SEC) issued guidance on its expectations for how publicly traded companies should address cyberattacks in their regulatory filings. The guidance does not change any existing rules, but clarifies that companies must include cybersecurity risks in their assessment of “the most significant factors that make an investment in the company speculative or risky.” In May EMC said it experienced “an extremely sophisticated cyberattack” that put its RSA SecurID tokens at risk as well as its corporate customers’ data security, and the SEC sent a comment letter asking the company how the cost of protecting itself against future breaches would affect its financial results. EMC’s chief accounting officer, Denis Cashman, replied that the costs did not have “a material impact” on financial results and therefore the company did not need to disclose it to investors, and that the company would continue to assess the effect of the attack and would “include a discussion of such impact as appropriate in future filings.” There are likely to be many more such exchanges with the SEC in the future now that the agency has spelled out its expectations. Many CFOs will continue to have some uncertainty about what to disclose, however, particularly just after a cyberattack when its impact is not fully clear. But the guidance states that companies should consider the cost of replacing stolen assets, repairing IT systems, implementing protection services, hiring third parties to repair reputation, and lost revenues from lost customers caused by the breach.

Fake Bank Site Spreads Malware **11/18/11, BankInfoSecurity.com**

The Office of the Comptroller of the Currency (OCC) last Thursday issued a warning about HelpWithMyBank.com, an illegitimate website feigning to offer consumer information about bank accounts and loans. Once visited, the HelpWithMyBank.com URL directs users to a legitimate consumer information site, HelpWithMyBank.gov, attempting to convince users they are connecting to a legitimate site, according to the OCC. But connecting to the fake site before the redirect is believed to expose consumers to malware.

Mobile Technology Changes Making Cyber Security More Difficult: Kroll **12/14/11, Business Insurance**

Kroll Inc.'s annual security forecast shows that security threats to mobile devices will reach record highs next year. In its report, which was released Dec. 14, Kroll noted that the demand and pressure that is being placed on some organizations to roll out mobile technologies for their employees is surpassing the ability of organizations to secure these devices. Cybercriminals know this, Kroll said, and are prepared to launch attacks using malware and malicious mobile applications. In addition, Kroll noted that the threat of attack involving social networking sites is on the rise, and that organizations should expect to see social media increasingly used in social engineering attacks. These attacks aim to convince users to divulge sensitive information or download malware. Finally, Kroll noted that cybercriminals will increasingly target small businesses, which are often unprepared for the risks and threats associated with the use of social media in the corporate environment.





COMMENTARY

“Have We Forgotten?” by P. Kevin Smith, CPP

With a beer in one hand and television remote in the other, I sat in my easy chair last weekend waiting for yet another NFL season to begin, no less excited than a 7-year old in line for a ride on Disney’s Space Mountain. I listened to Curt, Terry, Howie, Michael, and Jimmy break down the games as I made some last minute adjustments to my fantasy football team. Finally, the kick-off was at hand, and I saw stadiums around the country paying tribute to our fallen heroes from that horrific attack on American soil ten years ago. As I flipped through the channels, every broadcast showed huge flags covering the fields, with players, emergency responders, and military personnel joining hands to elevate the stars and stripes for the whole world to see. Emotional speeches were made, moments of silence were observed, and many tears were shed, in tribute to those who paid the ultimate sacrifice in our war against terrorism. Players and coaches wore symbols of national pride, and the theme of the day was the assertion that “we’ll never forget.” Wiping a tear from my cheek, it occurred to me that we in the financial services industry need to take a hard look in the mirror and ask ourselves, “Have we forgotten?”

In the wake of 9/11, security was first and foremost in everyone’s mind. Guards were hired, cameras were installed, x-ray machines scanned mail, access control systems were purchased, and the list goes on. Banks scrambled to purchase anti-money laundering software, knowing they would soon be responsible for monitoring customer transactions for potential terrorist financing. So severe were the heightened security reactions to these terrorist attacks, many of them bordered on ridiculous. Companies purchased thousands of water bottles and canned foods to be stored in preparation for the next attack. I even know of one security manager who was asked by his CEO to buy parachutes for the employees with offices on the top floor of their corporate headquarters. On the surface, the idea seemed plausible, until I learned that the building was only 12 stories tall. Security practitioners will tell you there’s nothing like a crisis event to grease the skids for a security business case, and the post 9/11 purchasing frenzy validated that theory. From the ridiculous to the sublime, security programs improved significantly after those planes crashed, and the financial services industry benefitted from that frenzy.

We were also summoned to assist our country in the fight against terrorism through the USA PATRIOT Act. I still marvel at the speed in which the Act was drafted and passed. Think about it, the attack occurred on September 11, 2001 and President Bush signed the bill into law on October 26, 2001, just 44 days after the attack. It’s hard to imagine our government working that quickly on anything, let alone legislation of that magnitude. The Act dramatically reduced restrictions on law enforcement to search financial information and paved the way for all financial institutions to “know their customers,” monitor transaction activity, and report any suspicious activity in a timely manner to the government. Like any legislation, the various laws and regulations emanating from 9/11 have a few quirks that make us wonder “how did that get in there,” but for the most part, they are sound business practices that most banks should have been following in the first place.

Still, as I watched players and coaches wear red, white and blue ribbons of “we’ll never forget,” I can’t help feeling that security is being shoved to the back of the bus. Business cases are getting harder to make in these difficult financial times, and I hear more stories of management questioning the need for security equipment upgrades, or even worse, staff replacements. Some banks have decided to eliminate fingerprinting and criminal history checks because the value doesn’t justify the expense. Others have reduced guard force operations because they haven’t had a robbery in over six months. The attitude toward security seems to be heading in the direction it was at the end of the 20th century, when it was viewed as a necessary evil. I hope and pray that it doesn’t take another 9/11 for management to recognize security as a critical piece of the business. In short, “let’s never forget”.





Profiles in Excellence – Mr. Terry Huskey, Wells Fargo Bank



Mr. Terry Huskey, CPP, CFSSP
Senior Vice President
Security Director, Southeast Region
Wells Fargo Bank

In this edition of our newsletter we are proud to highlight another member of the Banking and Financial Services Council. Terry Huskey is responsible for managing and directing all physical security activities in Well Fargo's Corporate Security southeast region.

He joined Wells Fargo in 1978 and has over 33 years of corporate security experience, including senior and executive level leadership positions in almost every facet of bank security and corporate investigations. Before that he was a commissioned officer in the U. S. Air Force for almost 30 years on active duty and in the reserves. He was a Special Agent and Special Agent in Charge with the Air Force Office of Special Investigations (AFOSI), with his final assignment as the Director of Investigative Operations.

He is widely recognized as an industry leader and the past chairman of the American Bankers Association (ABA) Bank Security Committee and the ASIS Banking and Financial Services Council . He is also the former international chairman and president of the International Association of Financial Crimes Investigators (IAFCI). He is a member and former chair of the North Carolina Bankers Association Bank Security Committee.

He graduated from the University of South Carolina, earning his bachelor's degree in IDS-Criminal Justice, and from Central Michigan University, earning his master's degree in business management. He holds several professional board certifications, including Certified Protection Professional (CPP) with the American Society of Industrial Security and Certified Financial Services Security Professional (CFSSP) with the American Bankers Association. He has received meritorious service awards from the Director of the Federal Bureau of Investigation and the Director of the U.S. Secret Service for his continued leadership and service in the financial security services industry.

