

ASIS Councils NEWSLETTER

Banking and Financial Services Council

Mr. Larry E. Brown – Chairman
First Citizens Bank & Trust

Mr. Terry Huskey, CPP – Vice Chair
Wachovia Corporation

Mr. Kevin O'Brien
The Bank of New York

Mr. Brian R. Abraham, CPP
3SI Security Systems

Mr. Robert S. Ballagh Jr, CPP
CheckFree

Mr. Steven K. Braden
Capital One Financial Corp

Mr. Michael J. Collins
Provident Bank

Mr. Robert D. Croskery
Wells Fargo & Company

Mr. Clark B. Cummings, CPP
FirstBank

Mr. Randy Dicampii
Wilmington Trust Company

Mr. Johan D. Du Plooy, CPP
Risk Diversion Pty Ltd

Mr. R. P. Handren, CPP
RBC Protection Services

Mr. Alexander Hilton
C.I.B.C.

Mr. Douglas W. Kohlsdorf, CPP

Mr. W. Joseph Majka
Visa USA

Mr. Richard L. Seba, CPP
JP Morgan Chase

Mr. Chris Smith
HBSC

Mr. P. Kevin Smith, CPP
Chevy Chase Bank

Mr. Francis X. Tesorero Jr, CPP
GE Consumer Finance

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

Mr. James W. Zardecki
Sovereign Bank

Banking and Financial Services Council

October – December 2009

It's That Wonderful Time of Year!!

Season greetings to all of our readers!! It's that wonderful time of the year! This season is particularly significant due to the challenging year we have faced in the banking industry. Nevertheless, it is a time for reflection and time to envision our future with hope, resilience, and determination. We cannot let circumstances dictate our future but rather boldly create it. This is the opportunity that is given to all of us at the beginning of a new year. On behalf of Larry Brown, our outgoing Council President and Terry Huskey, our incoming Council President, Happy Holidays and our best wishes for a prosperous New Year!!

ASIS International Quick Notes



CSOs Sought for Convergence Study

Has the integration of logical and physical security affected the culture within your organization? How? [Share your perspective with a doctoral researcher studying the cultural effects of convergence.](#)

Free downloads of the [ANSI/ASIS SPC.1-2009 Organizational Resilience: Security, Preparedness, and Continuity Management Systems—Requirements with Guidance for Use](#) standard.

ASIS Foundation introduces new **CRISP** report:

[Organized Retail Crime: Assessing the Risk and Developing Effective Strategies](#)
Alliance for Enterprise Security Risk Management Issues [Series of Complimentary Convergence and ERM Papers](#)

ASIS Upcoming Events



SEMINARS

2010

January 25-26: [Information Assets Protection Conference](#)

February 01-03: [ASIS Asia-Pacific Conference](#)

February 12-13: [CPP Classroom Review](#)

February 12-13: [PSP Classroom Review](#)

February 22-23: [Corporate Investigations](#)

February 22-26: [Physical Security: Introductory Applications and Technology](#)

WEBINARS

2010

January 27: [Understanding the Violent Mind in the Workplace](#)

February 17: [Web 2.0 Investigations That Move Beyond Google](#)



IN THE NEWS

The DHS Private Sector Preparedness (PS-Prep) Program and Standards **11/03/09, Continuity Central**

ASIS Commissioner Dr. Marc H Siegel describes the intent of the DHS PS-Prep Program as promoting "voluntary private sector preparedness." There are three standards identified for adoption as part of the PS-Prep Program, which are designed to represent distinct approaches for improving preparedness. However, ASIS supports a system in which businesses are not forced to choose among these three standards, but are permitted to develop voluntary standards that work best for their organization. Siegel argues that adoption or choice of any preparedness standard should not be about pursuing certification, but should be based on what makes the most sense in the context of an organization's business mission. In fact, Siegel maintains, third-party certification can be a barrier to small- and medium-sized businesses working to improve preparedness. In order to help businesses create a holistic approach to disruptive events, the ASIS Organizational Resilience (OR) Standard was developed. Now, ASIS and the British Standards Institution (BSI) have launched a joint development standard initiative. This new standard will not replace the OR Standard as they are two different standards. Additionally, neither the OR Standard or the new American National Business Continuity Management Standard is based on or contains content from the 2005 ASIS Business Continuity Guidelines, with the exception of several definitions.

Inside-Trade Probe Snares 'Octopussy' **11/06/09, Wall Street Journal**

Federal prosecutors have widened their crackdown on insider trading on Wall Street, in Silicon Valley, and other U.S. business hubs. A 24-page criminal complaint filed in New York federal court names 14 individuals who were allegedly part of an insider trading group that generated \$20 million in illegal profits. According to the complaint, the group included several hedge-fund traders, two lawyers, a former junior analyst at a credit-rating firm, and a technology-company executive. Five of those charged in the complaint have already pleaded guilty and have agreed to aid prosecutors in their investigation. Some of the elements of the group's operations were straight out of a James Bond movie, including packages of money, throwaway cell phones, and a central figure identified as "Octopussy," also known as Zvi Goffer, a former trader at the Galleon Group and the Schottenfeld Group. The government alleges that Goffer and his affiliates used nonpublic information to trade stocks of a number of companies, including Avaya Inc., 3Com Corp., Alliance Data Systems Corp., and Axcan Pharma Inc.

Eight Charged in Elaborate Theft of Debit Card Data **11/11/09, USA Today**

Eight foreigners were indicted by a U.S. grand jury on Nov. 10 for carrying out a massive computer fraud attack entailing the theft of debit card data from RBS WorldPay that was used to take millions of dollars from ATMs worldwide. Three of the eight cybercriminals allegedly broke into RBS WorldPay's computer network last November and cracked the encryption codes shielding account numbers and PINs for 44 prepaid payroll accounts. Acting U.S. attorney Sally Quillian Yates says the crooks boosted the payroll account limits, then arranged to have the stolen account numbers incorporated into the magnetic stripes of blank payment cards. A network of "cashers" proceeded to withdraw more than \$9 million from more than 2,100 ATMs in the United States, Canada, Estonia, Russia, Ukraine, Italy, Japan, and Hong Kong in just 12 hours. "The level of coordination was staggering," says RSA analyst Uri Rivner. He says the rapidity of the fraud attacks allowed an immense amount of theft to be perpetrated in a short time.





Alleged Ponzi Scheme Likely to Top \$1 Billion, FBI Says 11/13/09, Wall Street Journal

The FBI said on Nov. 12 that the Ponzi scheme Fort Lauderdale, Fla., attorney Scott W. Rothstein allegedly ran from 2005 until October likely topped \$1 billion, making it one of the largest Ponzi schemes discovered in the last several years. As part of that scheme, Rothstein--the founder of the high-profile Fort Lauderdale law firm Rothstein Rosenfeldt Adler P.A.--allegedly promised double-digit returns to clients who invested in what they believed were settlements related to sexual harassment and other labor-related claims. However, the stakes of the settlements Rothstein sold were actually fictitious. Rothstein also allegedly told investors that they could purchase the settlements at a discounted price and be repaid the full amount at a later time. Authorities say that Rothstein then used the funds he collected from new investors to pay off existing investors. Criminal charges are not expected to be filed in the case for the next several weeks.

Stickups and Burglaries Are On the Rise - at Work 11/16/09, Wall Street Journal

Corporate offices have seen an increase in robberies as traditional cash-heavy businesses, such as banks or convenience stores, have stepped-up security to avoid becoming targets during the recession. Many of these robberies involved small companies with ground-level offices that offer easy access for thieves. According to FBI statistics, the number of annual-reported burglaries increased 3.4 percent between 2004 and 2008. Sometimes the perpetrators are armed, heightening fear among office workers. Office thieves can be hard to detect at first glance. In the past year and a half, intruders got into Crosby-Volmer International Communications LLC's Washington, D.C., office three times during normal business hours. "All of these people had on ties and were wearing dress pants," says Robert Volmer, president of the public-relations firm. "People in offices tend to give [strangers] the benefit of the doubt." Volmer e-mailed a letter of complaint to the building's owner, Blake Real Estate Inc., in July but says he hasn't seen any signs of increased security. Stephen Lustgarten, Blake Real Estate's executive vice president, says, "The crime in that building would be no higher than any other urban environment in Washington. [Crosby-Volmer employees] left their back door open and unattended which is why they had a problem." After receiving the complaint e-mail, Lustgarten says the company briefed tenants on how to prevent future incidents by reminding them to be prudent, and avoid leaving personal items and entrances unattended. Crisis Care Network Inc. provided counseling to employees at 206 workplaces following incidences of armed robbery in the third quarter of 2009, a significant uptick from the 185 workplaces the company counseled during the same time in 2008.

Agencies Align Antifraud Efforts 11/18/09, American Banker

The Treasury Department, the Securities and Exchange Commission, the Department of Housing and Urban Development and Justice Department established a financial fraud task force on Tuesday. The task force, led by Justice and supported by the other agencies on a steering committee, will investigate and prosecute financial crimes, address discrimination in lending and financial markets and seek to recover proceeds for victims. It will build off of existing efforts to combat mortgage, securities and corporate fraud. The task force replaces the Corporate Task Force established in 2002. The attorney general will convene the task force's first meeting in the next 30 days. "The task force's mission is not just to hold accountable those who helped bring about the last financial meltdown, but to prevent another meltdown from happening," Attorney General Eric Holder said at a news conference. Treasury Secretary Tim Geithner reiterated that mission. "We are making clear that the Obama administration is going to act aggressively and proactively in a coordinated effort to combat financial fraud," Geithner said. "It's not enough to prosecute fraud only after it's become widespread. We can't wait for problems to peak before we respond."





Phishing scam spreads to three more states 12/07/09, Bank Info Security

Banking customers in three additional states have received bogus text messages purporting to be from their institutions. As part of a growing wave of similar phishing attempts throughout the nation, customers in Cincinnati, Ohio, St. Louis, Missouri and Lewiston, Idaho last week reported receiving text messages stating their bank accounts had been frozen. These attacks mirror those against bank customers in October in Pennsylvania, Nebraska and New York, and are part of a continuing wave of phishing attacks that have shot up 600 percent over last year, according to the Anti-Phishing Working Group. Law enforcement reported a number of banks had been targeted in the scam.

ATM fraud: new skimming scheme spreads 12/07/09, Bank Info Security

Three ATM skimming operations in Maryland, Illinois and Georgia have netted thieves more than \$120,000, according to law enforcement agencies investigating the crimes. These discoveries follow several recent incidents of ATM skimming in other states. Maryland State Police report that an ATM skimmer was placed on a Bank of America ATM in Eldersburg, Maryland, and that possibly \$30,000 was taken last week. Police have removed the skimmer, but say there could be more. State police have reported other incidents at various other banks in Northern Virginia and Maryland. Two men reportedly were photographed installing the skimming device, which collected card information from customers. The men then came back, removed the device, made counterfeit ATM cards with their stolen information and withdrew money.

CYBER SECURITY NEWS

FBI Warns of \$100M Cyber-Threat to Small Business 11/03/09, IDG News Service

A new FBI alert has been issued that warns small businesses, municipal governments, and schools about a significant increase in automated clearinghouse (ACH) fraud, in which cybercriminals are stealing millions of dollars from organizations through an ongoing cyber attack. As part of this attack, cybercriminals send an email to a business or organization's bookkeeper or financial officer that aims to trick them into downloading keylogging software. If the business or organization uses an online banking service, the cybercriminal can use the software to steal the victim's login credentials and create ACH transfers to "money mules," or people who are tricked into transferring the money overseas where it cannot be found. As part of the scam, cybercriminals also are launching distributed denial-of-service attacks against ACH processors in order to prevent them from recalling transfers before the funds can be sent overseas. The FBI says cybercriminals have attempted to steal roughly \$100 million through this scam. The bureau notes that cybercriminals are primarily attacking organizations that tend to work with smaller regional banks, which are often not capable of stopping the fraudulent ACH transfers. Compounding the problem is the fact that some banks do not have proper cybersecurity measures in place to protect against this attack, the FBI says.





Are Nations Paying Criminals for Botnet Attacks? 11/17/09, Network World

Countries that want to disrupt other nations' government, banking, and media resources can simply hire cybercriminals to launch botnet attacks, according to new report by McAfee that interviews 20 cybersecurity experts. McAfee's Dmitri Alperovitch says botnet attacks are hard to trace because of the anonymous nature of how they are requested and paid for. William Crowell, former deputy director of the U.S. National Security Agency, says that "anyone can go to a criminal group and rent a botnet. We've reached a point where you only need money to cause disruption, not know-how, and this is something that needs to be addressed." The July 4th, 2009, cyberattacks launched against South Korea and the United States prompted Rep. Peter Hoekstra (R-Mich.) to urge the United States to "conduct 'a show of force or strength' against North Korea for its alleged role in the attacks," the report says. Alperovitch says there is no concrete evidence that North Korea was behind the cyberattacks, but points out that it was unusual that the botnet was concentrated entirely in South Korea. Alperovitch also notes that North Korea gets its Internet link from China because North Korea never took ownership of the top-level domains it was assigned by ICANN. Countries that are known to be expanding their cyberwarfare capabilities include the United States, France, Israel, Russia, and China, according to the report. Major cyberconflicts have the potential to hurt businesses and individuals, indicating a need for greater public discussion about such issues.

FBI Suspects Terrorists Are Exploring Cyber Attacks 11/18/09, Wall Street Journal

Steven Chabinsky, the deputy assistant director of the FBI's Cyber Division, told members of the Senate Judiciary Committee on Nov. 17 that the bureau is investigating individuals with suspected ties to al-Qaida who seem to be interested in launching cyberattacks on computer systems that control vital pieces of the nation's infrastructure. Among the pieces of infrastructure that could be vulnerable to such attacks are power grids and transportation systems, Chabinsky said. He added that while the FBI has no evidence that terrorist organizations like al-Qaida have developed the ability to launch sophisticated cyberattacks, the lack of security in U.S. computer software systems makes it more likely that terrorists could launch attacks at some point in the future. Chabinsky also noted that if terrorists were to ever develop a capability to launch sophisticated attacks, those capabilities would likely be used with "destructive and deadly intent." Also testifying at the hearing was Associate Attorney General James Baker, who noted that the Obama administration is considering whether or not to try to change the laws that deal with technology and surveillance in order to better protect the nation from cyberattacks.

Restaurants Sue Vendor for Unsecured Card Processor 11/30/09, Wired News

Seven restaurants in Louisiana and Mississippi have filed a class-action lawsuit against Radiant Systems, the maker of a point-of-sale (POS) system that they say was not compliant with the PCI Data Security Standard (DSS). According to the plaintiffs, Radiant's Aloha POS system violated the PCI DSS because it stored all of the data embedded in the magnetic stripes of credit and debit cards after transactions had been completed. Also named in the lawsuit is retailer Computer World, which sold and maintained the Aloha POS system. The plaintiffs note that Computer World made them vulnerable to security breaches because it failed to secure a remote-access program that it installed on the Aloha POS system to allow its technicians to correct technical problems from off-site. The plaintiffs say that this allowed a hacker to access the POS system from at least 19 businesses, install malware on those systems, steal credit card data as cards were swiped, and send that data to a Romanian email address.





Restaurants Sue Vendor for Unsecured Card Processor 11/30/09, Wired News

Seven restaurants in Louisiana and Mississippi have filed a class-action lawsuit against Radiant Systems, the maker of a point-of-sale (POS) system that they say was not compliant with the PCI Data Security Standard (DSS). According to the plaintiffs, Radiant's Aloha POS system violated the PCI DSS because it stored all of the data embedded in the magnetic stripes of credit and debit cards after transactions had been completed. Also named in the lawsuit is retailer Computer World, which sold and maintained the Aloha POS system. The plaintiffs note that Computer World made them vulnerable to security breaches because it failed to secure a remote-access program that it installed on the Aloha POS system to allow its technicians to correct technical problems from off-site. The plaintiffs say that this allowed a hacker to access the POS system from at least 19 businesses, install malware on those systems, steal credit card data as cards were swiped, and send that data to a Romanian email address. The lawsuit seeks to recover millions of dollars in damages the plaintiffs say they incurred as the result of the breach, including fines for not being PCI compliant, the cost of forensic audits to determine the source of the breach, chargebacks to cover fraudulent charges made by criminals on customer accounts, and reimbursements to card providers who had to issue new cards to affected customers. Radiant says the allegations are without merit.

Survey Shows Cyberattacks Are Getting More Disruptive 12/01/09, NextGov.com

Cyberattacks powerful enough to break through computer networks and interrupt online business services are increasing precipitously, according to a recent Computer Security Institute survey of public and private sector IT professionals. Infections from software built to break into or damage a computer system were "easily the most prevalent" type of cyberattack this year, the survey found. Nearly two-thirds of the 443 respondents said they had experienced malware attacks in 2009, compared to 50 percent the previous year. Frequently these attacks were implemented in multiple stages, in which the malware downloaded different tools to exacerbate the severity of the contamination once inside the network. Eight percent of survey participants were employed by the federal government. Reports of malware infection are likely to continue increasing as hackers "spend more energy customizing malware to make it more effective in targeted attacks," the survey's report said. Twenty-five percent of survey respondents said targeted attacks were involved in at least some of their security instances, and 4 percent said they had witnessed 10 or more such intrusions.

Scammers scrape RAM for bank card data 12/09/09, The Register

In the wake of industry rules requiring credit card data to be encrypted, malware that siphons clear-text information from computer memory is all the rage among scammers, security researchers say. So-called RAM scrapers scour the random access memory of POS, or point-of-sale, terminals, where PINs and other credit card data must be stored in the clear so it can be processed. When valuable information passes through, it is uploaded to servers controlled by credit card thieves. While RAM scrapers have been around for a few years, they are a "fairly new" threat, according to a report released Wednesday that outlines the 15 most common attacks encountered by security experts at Verizon Business.

