

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
Canadian Imperial Bank

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 January – March 2009

ASIS International Quick Notes

ASIS Foundation Report Helps Managers Plan for Change

The ASIS Foundation has released "[Planning for Change: Security Managers' Perspectives on Future Demographic, Crime and Technology Trends](#)," a report that provides concise descriptions of predicted demographic, crime and technology trends in the United States. The report also summarizes how experts anticipate these changes will influence security over the next five to 10 years, and offers practical recommendations security managers can adopt now to address these anticipated trends.

The ASIS Foundation contracted the Urban Institute, a non-profit, non-partisan social policy and economic research organization, to forecast demographic and crime trends and to provide guidance for the emerging security challenges that may arise from such predictions. The resulting 51-page report predicts that the U.S. security industry will face many challenges, including an aging workforce, an increasingly diverse population and a growth in high-tech crimes.

ASIS Upcoming Events



SEMINARS

[March 30-31: Corporate Investigations](#)

[April 3-4: Physical Security Professional \(PSP®\) Classroom Review](#)

[April 3-4: Professional Certified Investigator \(PCI®\) Classroom Review](#)

[April 3-4: Certified Protection Professional \(CPP®\) Classroom Review](#)

[April 6-8: Managing Your Physical Security Program](#)





[April 24-30: ASIS International ISO 28000 Lead Auditor Certification Course](#)

[May 4-7: Assets Protection Course II: Practical Applications](#)

[June 15-16: Corporate Investigations: How to Conduct Proper and Effective Internal Investigations](#)

[June 15-17: Facility Security Design](#)

[June 15-18: Assets Protection Course III: Functional Management](#)

[June 17-18: Safeguarding Information Assets in the Ever-changing Business Environment](#)

[June 23-24: Securing the Pharmaceutical Supply Chain - Manufacturer to Consumer](#)

WEBINARS

[April 15: Getting the Boss to Listen to You](#)

[April 24: Certification 360: Strategies and Techniques to Evaluate and Improve Your Certification Preparation Program](#)

[May 20: Conduct Your Best Video Site System Survey](#)

[June 17: Understanding Body Language: Recognizing the Hidden Meaning of the Unspoken Dialogue](#)

In The News

CheckFree Warns 5 Million Customers After Hack IDG News Service, 01/06/09, McMillan, Robert

CheckFree and some of the banks that use its services are notifying more than 5 million customers about a Dec. 2 attack in which cybercriminals tried to steal passwords from their victims' computers. The attack began when hackers sent phishing emails to CheckFree that apparently tricked employees into divulging the company's password with its domain registrar. The attackers then used the password to log into CheckFree's account with the registrar and change the DNS settings for its Web sites. This allowed attackers to reroute the customers who visited CheckFree's Web sites during a nearly 10-hour period on Dec. 2 to a Ukrainian Web server that used malware to try and install a password-stealing program on their computers. CheckFree's parent company, Fiserv, says roughly 160,000 consumers were exposed to the Ukrainian site, though only those who did not have antivirus software and were using an old version of Adobe Acrobat were infected. But since the company lost control over its Web domains, it does not know exactly who was affected, which means that it must warn a much larger number of consumers. The attack could have been much worse considering the fact that CheckFree processes bill payments for more than half of all U.S. banks, says Gartner analyst Avivah Litan.





Wall Street Crisis Brings Lax E-Discovery Law Enforcement to Light, 01/14/09, Computerworld

The financial crisis on Wall Street has prompted numerous investigations into the lending practices of financial services firms, all with a similar focus: Who knew what, and when did they know it? Strong electronic records retention plans could help users quickly answer such questions. However, industry observers note, few of the records-retention regulations enacted over the past decade have been strongly enforced, and most companies have done little to comply with them. Analysts warn that the fallout from the Wall Street meltdown will lead quickly to stronger enforcement of existing laws, including the Sarbanes-Oxley Act, the Electronic Signatures in Global and National Commerce Act, the U.S. Security and Exchange Commission's Rule 17A-4, and the Gramm-Leach-Bliley Act, and perhaps some new ones targeting the financial services industry. As of January 14, only 10 percent to 15 percent of U.S. corporations have electronic records retention systems in place, according to Gartner Inc., a consulting firm "In terms of a good electronic records systems, I would say it is closer to zero," said Gartner analyst.

RBS WorldPay: ATM Heist Nets \$9 Million in 30 Minutes, 02/04/09, Finextra

RBS WorldPay, the U.S. payments processing arm of Royal Bank of Scotland Group, allegedly lost \$9 million in a 30-minute period during a global ATM heist that involved 100 cloned cards in 49 cities worldwide. RBS first reported a breach of its computer systems and the fraudulent use of 100 cards in a press release that was issued on December 23, 2008. The bank confirmed that an unauthorized party had improperly accessed its computer system in November 2008 and that the personal information of 1.5 million pre-paid cardholders had been compromised. So far, the FBI has no suspects and has made no arrests in this scam. An attorney in Atlanta has filed a class-action lawsuit against RBS WorldPay for allegedly failing to protect personal information.

Bellevue Man Charged in \$65M Pyramid Scheme, 02/06/09, Seattle Times

A Bellevue businessman who allegedly ran a \$65 million pyramid scheme involving investments in Southeast Asian oil development has been ordered held in federal custody by a U.S. magistrate judge after his arrest on February 5. Prosecutors allege that the 48-year-old suspect and two Malaysian men used money they took from some investors to pay others; all the while claiming they were helping develop vast tracks of oil-rich land overseas. The suspect was arrested at his Eastside home on February 5. He faces a 23-count indictment that could land him in federal prison for decades. He is charged with conspiracy, mail fraud, wire fraud, money laundering, and tax evasion.

Bank Fraud Mastermind Arrested, 02/10/09, Bradenton Herald

The accused mastermind of an \$83 million bank-fraud scheme involving land sales in Manatee and Sarasota counties has been arrested in Jordan, a federal prosecutor said on February 9 during the trial of a co-defendant. The defendant is accused of buying seven parcels for \$43 million, reselling them to the co-defendant and others for \$117 million and helping the buyers obtain \$83 million in bank loans.





Heartland Data Breach Update: Now More Than 150 Institutions Impacted, 02/11/09, BankInfoSecurity.com, McGlasson, Linda

At least 157 financial institutions were affected by the security breach on Heartland Payment Services' authentication system last year, reveals a recent survey by the Independent Community Bankers of America (ICBA). More than 80 percent of the 512 institutions that responded to ICBA's survey said they had either credit and/or debit cards affected by the Heartland breach. Just 13 percent of the responding institutions said they still didn't know if their customers' card accounts were compromised in the breach. Among those most affected by the incident was Jackson, Miss.-based Trustmark Bank, which had 75,000 of its cards compromised in the breach; Raleigh, N.C.-based State Employee's Credit Union, which had 56,000 of its cards compromised; and El Paso, Texas-based GECU, which had 25,000 of its cards compromised. Heartland says that a variety of information associated with those cards was stolen in the breach, including account numbers, expiration dates, and some customer names.

Fugitive Financier Arrested at U.S. Border, 02/12/09, Associate Press

An American fugitive accused in a \$100-million mortgage fraud was caught at the Canadian border. The suspect is the second of three fugitives to be caught in the investigation of Loomis Wealth Solutions, an investment company based in Roseville, California, and several related companies. Court documents say they had defrauded investors and mortgage companies of \$100-million since 2006. The deals involved 500 homes and condominiums in California, Florida, Nevada, Illinois, Colorado and Arizona, Internal Revenue Service affidavits said.

Financial Crisis Called Top Security Threat to US, 02/13/09, Washington Post, Pincus, Walter; Warrick, Joby

During a nearly two-hour congressional hearing on Thursday, Director of National Intelligence Dennis C. Blair told lawmakers that for the first time in six years, terrorism is not the most immediate security threat to the United States. According to Blair, the threat posed by terrorism has now been supplanted by a variety of threats that could be created by the economic turmoil sweeping the globe. In his remarks before the Senate Select Committee on Intelligence, Blair said that the most immediate effect the recession will have on the United States would be allies not being able to fully meet their defense and humanitarian obligations. In addition, the number of refugees from the Caribbean could increase because of the economic turmoil. However, the recession could also create more dire threats such as "high levels of violent extremism," similar to what was seen during the Great Depression, Blair said, adding that there could also be "regime-threatening instability" in some countries if the recession lasts for another one to two years. Yet despite the threat posed by the recession, Blair said he was not refocusing the intelligence community's basic collection and analytic work away from terrorism and nations such as Afghanistan, Pakistan, Iran, North Korea, Russia, and China.



CYBER SECURITY NEWS

Data Breaches Up Almost 50 Percent, Affecting Records of 35.7 Million People, 01/06/09, Washington Post, Krebs, Brian

The number of data breaches rose almost 50 percent in 2008 compared to the year before, compromising the personal records of at least 35.7 million Americans, says the Identity Theft Resource Center (ITRC). ITRC says that 656 breaches were reported last year, versus 446 in 2007. Approximately 37 percent of the breaches targeted businesses, while the segment of breaches attributed to data theft from current and former employees rose from 7 percent in 2007 to close to 16 percent in 2008. "This may be reflective of the economy, or the fact that there are more organized crime rings going after company information using insiders," says ITRC's Linda Foley. She says that many businesses fail to disclose data breaches even though 45 states have rules that consumers must be alerted of any loss or theft of private records.

Phishing Attack Disguised as Message from FDIC, 01/15/09, Central Valley Business Times

The Federal Deposit Insurance Corporation (FDIC) reports fraudulent e-mails claim that a phishing attack has affected the Fedwire system and that restrictions are in place. The e-mails further instruct recipients to click on links within the e-mail for additional information. That is where the trouble starts. Once clicked, the links actually unleash malicious Trojan horse programs onto end users' computers. The real FDIC says consumers, businesses, and financial institutions should be aware that Fedwire operations are not restricted and are operating as normal.

Data Scams Have Kicked into High Gear as Markets Tumble, 01/29/09, USA Today

Cybercriminals have launched a massive new wave of Internet-based schemes to steal personal data and carry out financial scams in an effort to take advantage of the fear and confusion created by tumbling financial markets, security specialists say. The schemes, often involving online promotions touting fake computer virus protection, get-rich scams and funny or lurid videos already were rising last fall when financial markets took a dive. With consumers around the world panicking, the number of scams on the Web soared. The number of malicious programs circulating on the Internet tripled to more than 31,000 a day in mid-September, coinciding with the sudden collapse of the U.S. financial sector, according to Panda Security, an Internet security firm.

"A New Internet?", 02/15/09, New York Times, Markoff, John

There is a growing belief among engineers and security experts that the only way to fix Internet security is to recreate the Internet from scratch. What a new Internet might look like is being discussed, but one possible solution would create a "gated community" in which users would relinquish their anonymity and certain freedoms in return for safety, which is already the case for many corporate and government Internet users. As more secure networks are created, the current Internet will continue to become an increasingly dangerous area that legitimate users will want to avoid. "Unless we're willing to rethink today's Internet," says Nick McKeown, a Stanford University engineer working on building a new Internet, "we're just waiting for a series of public catastrophes." Last year, a malicious software program believed to have been released by a criminal organization in Eastern Europe infected more than 12 million computers after bypassing the world's best cyber defenses.

