

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 Dicampfi
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 – February 2008

The B&FS Council is off to a Great Beginning in 2008!!

The banking and Financial Services Council is off to a great start with its new Chair Larry Brown and Vice Chair Terry Huskey, CPP. Both Larry and Terry are well seasoned security practitioners in the banking and financial arena and the council looks forward to their leadership. We wish them both all the best as they assume their new roles. Our heartfelt gratitude goes to Kevin O'Brien for his tireless efforts in leading the Council during the last terms. Kevin, we thank you for your leadership, professionalism, friendship, and for making a true difference!

In The News

International Gang Hacks Into Texas Bank Biloxi Sun Herald (MS) (01/25/08) P. C7 ; Shlachter, Barry

Hackers gained access to OmniAmerican Bank's records, stealing account numbers, creating fake debit cards and creating new PINs. They then used the debit cards to withdraw cash from ATMs in Eastern Europe, Britain, Canada and New York. OmniAmerican, which operates 17 branches in Texas, responded by limiting account access to Texas and cutting the maximum ATM withdrawal in half from Jan. 18-20. Bank officials said that less than 100 accounts were compromised and a "minimal" amount of money was stolen. No bank customers will lose any money, and the bank plans to issue almost 40,000 new debit cards to protect customers against any additional fraud. A security expert said that the attack was pulled off by a sophisticated group of cyber criminals, most likely hailing from Russia or China.

Bank Robberies On the Rise Chattanooga Times Free Press (TN) (01/12/08) ; Williams, Amy O.

The FBI reports that bank robberies are on the increase in East Tennessee and other areas of the country. FBI authorities note that the majority of bank robberies take place at branches prior to noon during the workweek. Over 50 percent of those robbers ask for money with a written note and say they have a weapon, although just one-eighth of them bring out a gun, knife, or bomb. During 2006, there were 17 of these crimes in the Chattanooga region. Across the United States, though, there were 7,000 crimes for that period. Thieves got away with \$72.7 million, and law-enforcement just recovered \$11.2 million of that amount. In Chattanooga, the FBI says banks lost \$295,000 to thieves. While bank officials do not like to talk about specifics, many institutions employ high-tech security equipment, including cameras, money outfitted with electronic trackers and dye packs, and silent alarms.

Treasury Plans Social Security Debit Card Wall Street Journal (01/04/08) ; Laise, Eleanor

The Treasury Department is ready to introduce the Direct Express debit card, a prepaid debit card for Social Security and Supplemental Security Income recipients who do not have a bank account. The card is a component of a broader Treasury initiative to migrate to electronic payments. "We've been working for a while to try to understand the needs of the unbanked," says Treasury's Judith Tillman. "Combine that with problems we've seen with financial crimes and identity theft, problems with forged checks and stolen checks and so on, the debit card seemed like the right answer." Comerica Bank will serve as the card's issuer, and the card will debut in a handful of states in the spring and be rolled out nationwide by the end of the summer. Cardholders would have faster access to their money and avoid stolen checks and other security problems, while Treasury and banking experts say the product could yield substantial cost savings for beneficiaries and the federal government. Social Security retirement, disability and survivor benefits, and SSI benefits will be automatically loaded onto the card account on the designated payment day for beneficiaries who sign up for the debit card, which can be utilized at bank branches, retail sites, ATMs, and online. Cardholder fees, interchange fees when cardholders employ the card at the point of sale, and the float on funds sitting in cardholders' accounts will earn money for Comerica.

How New Authentication Systems are Altering Fraud Picture American Banker (12/27/07); Wolfe, Daniel

In 2007, all financial institutions were required to make progress toward establishing robust authentication to prevent online fraud, and the initiative seems to have been quite successful. By October 2007, 80 percent of U.S. banks had fulfilled the Federal Financial Institutions Examination Council's mandate that customers gain access to online banking using more than just a user name and password, reports research firm TowerGroup, and an additional 15 percent of U.S. banks were found to be closing in on the goal. Initial findings reveal that between 2006 and 2007, fraud in the U.S. online channel has dropped by 30 percent to 40 percent, "specifically due to implementing the FFIEC-required authentication," says George Tubin of TowerGroup. However, bankers must now grow more vigilant in protecting other channels, as scammers are seeking weaknesses in other areas. For example, the number of branch and contact center fraud incidents is on the rise, says Tubin. Avivah Litan of Gartner praises the FFIEC regulations, which have caused the percentage of account takeovers to fall by 15 basis points over the past six months, according to Litan's estimate. Nevertheless, Litan concurs that criminals are switching tactics and, instead of commandeering accounts online, are using data obtained from phishing to open accounts at banks with feeblers defenses.

Atlanta: Bank Heist Capital of Nation" CNN (12/17/07) ; Smith, Tristan

Atlanta, Ga., reported 350 bank robberies, the most in the nation, between October 2006 and October 2007, according to an annual report by the FBI. Although there were 122 armed robberies reported, most of Atlanta's bank heists were "note jobs," where the thief implies that they are in possession of a gun without making it visible. ATM heists and nine armored car robberies were factored into the total number of reported robberies. The FBI said that the increased number of bank robberies in Atlanta illustrates a rise in violent crime across the nation, especially in major urban areas. Atlanta has also seen its population grow dramatically over the past decade, leading to the opening of more banks in the metropolitan area. The Georgia Bankers Association said that the average amount stolen in a bank heist is only between \$2,000 and \$3,000.

Corporate Crime on the Rise London Free Press (Canada) (12/17/07) ; Musgreave, John; Porter, Graham

Losses stemming from corporate crime have increased substantially over the last two years, though the majority of companies have faith in their existing fraud controls, according to results from PricewaterhouseCooper's (PwC) 2007 global economic crime survey. The poll revealed that 43 percent of international survey respondents experienced corporate crime in 2007, and that their reported losses due to crime grew from \$1.7 million in 2005 to \$2.4 million in 2007, on average. Nevertheless, roughly half of the global companies polled believe it is "very unlikely" that they will suffer from corporate crime in the near future, says Bruce Webster of PwC. This perspective suggests that many organizations are insufficiently aware of the danger of corporate fraud. And while over 60 percent of Canadian companies surveyed have enhanced their security controls since 2005, 67 percent of those companies still lack fraud-related training programs, and 36 percent have not instituted a "whistleblower" hotline. Without such anti-fraud controls, companies put themselves at risk for economic crime and decrease the odds of detecting fraud, says Webster. Indeed, almost 40 percent of corporate crime incidents reported by Canadian businesses were discovered by chance. The survey also revealed that 30 percent of reported international fraud incidents were cases of asset misappropriation, which is the easiest type of fraud to identify; however, many businesses do not see asset misappropriation as a threat. Also, employees were to blame for the most grave fraud transgressions, according to 67 percent of victimized Canadian companies.

CYBER SECURITY NEWS

There Are Some Security Threats You Can Worry Less About InfoWorld (12/28/07) ; Snyder, Bill

In 2007, levels of virus-embedded email and image spam dropped. Compared with 2006, IronPort Systems notes that email attachments with viruses embedded decreased by about half, estimating attacks at about 450 by the year's end. Since 2005, image spam has been a formidable cyber threat, yet levels of this kind of attack also dwindled in 2007. Along with Symantec and McAfee, IronPort reported that improved spam detection filters have led hackers to divert their attacks from email attachments to other platforms such as photo-sharing Web sites. Cyber attacks targeting business applications and URL viruses have spiked by 50 percent to 60 percent and at least 250 percent, respectively. "Traditional viruses have been around for years, a long enough time to harden defenses against malicious attachments," says IronPort product manager Dave Mayer. The statistics from 2007's Web threats indicate that although some strategies for launching viruses have declined, hackers are relying on other executable measures to successfully launch their attacks.

New Trojan Preys on Commercial Banking Customers Register (UK) (12/17/07) ; Goodin, Dan

A new virus, the Prg Bank Trojan, is victimizing commercial bank customers by logging into their online accounts and transferring funds to accounts owned by cyber criminals. So far, the virus is known to have attacked commercial banking clients at 20 banks and could have cost customers as much as \$1 million. The Prg Bank Trojan usually comes to commercial banking customers as an email, supposedly from their bank, leading consumers to click on an infected link. Once the user's system is infected, the hacker is notified every time a user initiates a transaction, allowing criminals to bypass a bank's online security system.

Information Security Standards Risk Management (12/07) Vol. 54, No. 12, P. 11 ; Lindenmayer, Gerhard

For many organizations, the most essential asset is information, which means organizations must implement security measures to ensure data is not inadvertently or maliciously compromised. Certain best practices exist for securing network data. A layered approach--which combines technology, policy, training, and enforcement--is the best way to achieve full protection. Encryption, antivirus software, and firewalls are key technological elements of data security. Adopting an intrusion detection system helps safeguard the network infrastructure and notifies the IT department when problems occur. In addition, it is crucial to train employees regarding the data in their control and to enforce a robust password policy. Workers should have a limited ability, if any, to use memory sticks, CD/DVD drives, and other portable USB storage devices; though strict, this policy will prevent data from being carried away from the premises. Restricting workers' Internet access to work-related sites also keeps the network safe from viral downloads. Finally, it is important to have outside consultants conduct regularly scheduled patches and yearly penetration tests. Businesses that utilize credit cards for online transactions should scan their servers and ports at least four times each year to adhere to the Payment Card Industry Data Security Standard.

How to Avoid the Next Data Breach eWeek (12/21/07) ; Markovich, Slavik

There are several steps organizations can take to reduce the risk of data breaches and mitigate the impact of the ones that do happen. One thing that organizations can do is to make sure that they have developed a security policy that takes into account what data assets need to be protected, the threat landscape, and the possible consequences of a security breach. This policy should be communicated to employees and revised periodically. Next, organizations should determine where their sensitive data assets are and move to control access to this data. Unauthorized copying, printing, and backup-making should be prevented. In addition, both data in motion and data at rest should be encrypted. Finally, organizations should regularly use automated tools to find bad component configurations, weak passwords, and vendor defaults in databases, application servers, routers, and other devices.

Scary Tech Stories: How Dangerous User Behavior Puts Networks at Risk Network World (12/10/07) ; Dubie, Denise

For many IT managers, users' actions--whether unintentional or intentional--can produce nightmarish security situations. Steve Moore of Mary Kay Cosmetics explains, "End users are smarter than ever," thanks to home PCs and information on the Internet. According to new research from the Ponemon Institute, more than half of users knowingly flout corporate security standards. And, through routine behaviors, trusted insiders "create data exposures of extraordinary scope," according to poll data from RSA. Consequently, IT executives struggle to balance safeguarding data from inappropriate use with expanding access to information as needed. Password security is one major area of concern, as many end users neglect to update their passwords, failing to realize that technology exists that can exploit their passwords to obtain information and corrupt the network. Even technology-savvy users without malicious intent can cause trouble, such as those who attempt to deploy consumer wireless routers at work, an action that creates security gaps on the network, says Martin Webb of Canada's Ministry of Labour and Citizens' Services. Mobile devices such as USB flash drives and thumb drives also enable workers to take too much data off corporate networks. Such workers may simply be trying to complete projects at home but, by circumventing security policies, are putting the network at risk.