ASIS Councils NEWSLETTER

Banking & Financial Services Council April - June 2013

Special points of interest:

- Article on Social Engineering
- New Council Member Spotlight

Inside this issue:

Social Engineering	1
New Council Member Spotlight	2
ASIS Professional Development Programs	3
In The News	4
Cyber Security News	7
Council Membership	8
Pre-Seminar Workshop Agenda	8

Social Engineering

What is social engineering?

Social engineering is essentially the art of gaining access to buildings, systems or data by exploiting human psychology, rather than by breaking in or using technical hacking techniques. For example, instead of trying to find a software vulnerability, a social engineer might call an employee and pose as an IT support person, trying to trick the employee into divulging his password.

How are companies at risk?

Social engineering has proven to be a very successful way for a criminal to "get inside" your organization. Once a social engineer has a trusted employee's password, he can simply log in and snoop around for sensitive data. Another try might be to scam someone out of an access card or code in order to physically get inside a facility, whether to access data, steal assets, or even to harm people.

Penetration example using social engineering.

In one penetration test, an ethical tester used current events, public information available on social network sites, and a “vendor” shirt he purchased at a thrift store to prepare for his illegal entry. The shirt helped him convince building reception and other employees that he was a vendor employee on a technical support visit. Once inside, he was able to give his other team members illegal entry as well. He also managed to drop several malware-laden USBs and hack into the company's network, all within sight of other employees.

Tips for recognizing social engineering.

To avoid falling prey to social engineering, employees should ask the following questions:

- Was I expecting this phone call?
- Was I expecting this visitor?
- Was I expecting this email?
- Do I know and trust the caller, visitor or sender?
- Are they asking me to divulge personal information?
- Are they asking me to divulge company information?
- Are they asking me to divulge information about our clients or other vendors?
- Does the email contain “suspicious” links, misspellings or look generally unprofessional?

Social engineering awareness.

These are just a few brief examples of social engineering tactics and recognition tips. Information security officers, physical security officers, management and other key resources for companies must partner to develop comprehensive social engineering awareness campaigns to combat this risk.

For more information and awareness tips for social engineering, the “Ultimate Guide to Social Engineering” may be downloaded from www.CSOonline.com.

New Council Member Spotlight

The ASIS Banking & Financial Services Council would like to welcome Gary Reynolds as one of the newest members of the council.

Gary Reynolds is the Senior Vice President and Corporate Security and Investigations Director for Union Bank where he is responsible for the development of effective strategies to mitigate risk, maintain continuity of operations, and safeguard the organization.

Prior to Union Bank, Gary was the Chief Security Officer for Dragnet Solutions, Inc., with responsibilities for business development, physical, and logical security.

Previous to joining Dragnet Solutions, Gary held the position of SVP/Director of Financial Crime Investigations at Wells Fargo Bank. With a team of 60 investigators, Gary headed all aspects of external fraud crimes aimed at the bank. He managed the electronic crime investigation team overseeing outsider/insider attacks, forensic investigations, and electronic discovery. Prior to joining Wells Fargo, Gary spent 20 years in county and municipal law enforcement retiring from the Santa Rosa Police Department.

" Banks are an almost irresistible attraction for that element of our society which seeks unearned money"

- J. Edgar Hoover

Gary holds a B.A. degree from the University of Redlands, and a MS degree from Utica College of New York, where he is currently an adjunct professor teaching at the graduate level in the Economic Crime Program. He is also on the staff at the Santa Rosa Junior College Public Safety Training Center where he teaches Unusual Incident Management at the basic academy.

Gary is a Certified Fraud Examiner, Certified Anti Terrorism Specialist, and holds a Certificate in Computer Forensics from Oregon State University. He is a licensed private investigator and current member of the International Association of Bomb Technicians and Investigators.

Gary is a nationally recognized speaker on identity theft and financial crime. His speaking assignments have included, The California Identity Theft Summit, Federal Deposit Insurance Corporation Identity Theft Symposium, Federal Financial Institutions Examination Council Conference, IRS Identity Theft Roundtable, ING Identity Theft Conference, and the Ameriprise Identity Theft Conference.

Published papers: Facial Recognition: A Biometric For The Fight Against Check Fraud

ASIS
INTERNATIONAL
Advancing Security Worldwide®

Upcoming ASIS Events

ASIS 2013

ASIS INTERNATIONAL
59TH ANNUAL
SEMINAR AND EXHIBITS

SEPTEMBER
24–27

McCORMICK PLACE, CHICAGO, IL

REMINDER:

If you haven't yet registered for this year's seminar and exhibits, go to:

www.asisonline.org

ASIS Professional Development Programs & Webinars

July 15 - 16, 2013 - **Executive Protection**

July 15 - 18, 2013 - **Managing Your Physical Security Program and Advanced Topics**

July 17 - 18, 2013 - **Security Program Design - A Critical Infrastructure Protection Model**

July 17, 2013 - **Recognizing & Assessing Suspicious Indicators**

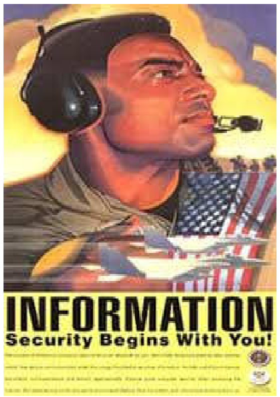
July 24, 2013 - **High-Rise Class "A" Security Service**

July 25, 2013 - **Practical Applications of Video Analytics**

August 7, 2013 - **The Art of Security Leadership: How to Build Successful Risk-Based Security Programs (Without a Budget)**

August 21, 2013 - **Effects Based Security: Optimize Manpower and Budget**

You will find full course descriptions, locations & registration information at: www.asisonline.org



"Let us not look back in anger or forward in fear, but around in awareness."

- James Thurber

In the News

Sage Conversations: Taking a Holistic View of Security Operations 04/22/13, SecurityInfoWatch.com

Often within the security functions of public and private organizations there is a tendency to focus inward, missing the holistic perspective of how security benefits the greater organization mission. In an interview with Benjamin Butchko, CEO of Butchko Security Solutions, The Sage Group's Ronald Worman notes four major data elements that Butchko says could be used to create an information data model and architecture for security. These elements are: business data, such as facility, personnel and identity, and contracts management; physical security data, such as access control, intrusion, video surveillance, and voice; operations data, including SCADA, core process or workflows, raw materials, product stores, and locations; and the safety environment, such as proper certifications, medical clearances, and travel. Butchko argues that if this information was identified, captured, and organized properly, then it could be persistently evaluated in context of reactive and proactive analysis, and would equip the organization to spot trends that could tell leaders how to improve their operation, and also predict future events. Butchko is helping his clients by developing an interoperable leadership platform that aims to leverage the knowledge and resources of multiple security stakeholders, including technology vendors, software companies developing in Windows, SQL, and Sharepoint, device companies, and integrators. Another example of this new leadership mindset in the security industry can be found in the Security Executive Council (SEC). Several members of the council have created a Next Generation Security Leader Program that aligns with these leadership elements. Worman notes that this organization keeps a true external and internal perspective by identifying all-hazards risk and best practices that can be accessed through their Collective Knowledge database and consulting network to the accreditation of risk, resilience, and security solutions and services through their Solution Innovation Program (SIP).

The CSO Perspective on Risk Management 05/09/13, Help Net Security

Candy Alexander, CSO at Long Term Care Partners and member of the International Board of Directors for ISSA, in a recent interview gave her perspective on the value of risk management, threat mitigation, and security awareness. She says risk management programs should be simple, and should accomplish these three goals: identify real risks to the important items within the company; mitigate the risks; and continuously monitor the environment. Doing this properly, she says, involves talking with the business to understand what they see as critical to their operation, and then focusing on areas within the environment where the important things are. Regarding the evolving role of the CSO and the job market for aspiring security professionals, Alexander says it is important to be flexible and to stay current with technology and how it is being used. She uses bring-your-own-device (BYOD) as an example of a trend that security professionals ignored for a long time, to their detriment, before finally acknowledging. "You need to keep your ear to the ground and know what's going on as quickly as possible," she says. "Build trusted relationships with as many people as you can -- often times I have found out what's going on from my 'informal/off the record' conversations." Because it is not realistic to address all potential security risks, Alexander says risk management programs must focus on protecting what matters. Security awareness and training are important, but these should be limited to only what pertains to an individual's job function. "People get overloaded with information as it is, so providing security messages based on role or function is key. A consideration is to be sure to provide examples of 'why' it is important. People want to do the right thing, so if they know why they must use a certain safeguard -- they will," Alexander notes. As a final piece of advice to CSOs handling business issues surrounding risk management, she urges them to continue building relationships with other people -- get to know what their goals are and what their business processes are, in order to carry out a thorough and accurate risk assessment.

Banks Eye Voice Biometrics to Verify Customers 05/09/13, Wall Street Journal

Financial services companies like Barclays, Vanguard Group, and TD Waterhouse have started to deploy voice-recognition software to identify customers when they call customer service centers. While the technology to do this has been around for a while, it has only recently become accurate enough for more mainstream use.

Security is not for the passive!

"Voice biometrics to verify customer identity?"

Better be despised for too anxious apprehensions, than ruined by too confident security.

-Edmund Burke

Pa Houa Vue was arrested for stealing funds from a dead customer's bank account.

- The Columbian

"IP Theft Costs US $300 Billion Per Year"

Bank bans hats, sunglasses and hoods.

In The News (cont.)

Banking executives say the use of such systems can reduce fraud and improve customer service. Voice-recognition systems are widely viewed by those in the banking industry as more secure alternatives to password protection and more convenient than asking customers a series of security questions. Also called voice biometrics, the systems analyze characteristics of a person's speech like pitch, tone, and rhythm, by requiring the customer to give a voice print. This usually involves the customer repeating numbers, letters, or a phrase. The voice biometrics system Barclays uses requires a customer to talk naturally with a customer service representative for about 20 to 30 seconds while his or her identity is verified by the software. If the system is unable to verify the customer, the customer service representative will begin to ask security questions. Many other financial institutions have started using a similar approach. Gartner Vice President Avivah Litan said voice biometrics are currently 80 percent reliable. She said traditional methods of identifying customers, such as using security questions, have a 10 to 15 percent failure rate, largely because customers often forget the information they previously supplied.

Longwood Banks to Ban Hats, Sunglasses and Hoods, Cops Say 05/13/13, Orlando Sentinel (FL)

Police in Longwood, Fla., said that many banks in the city are that banning customers from wearing hats, sunglasses, and hoods in response to the growing number of bank robberies in Central Florida. "The simple act of removing hats, hoods and sunglasses in Longwood financial institutions will make it much easier to identify and capture anyone committing a crime," the Longwood Police Department said in a statement. The police hope the new policy will help deter so-called "Note Job" robbers, who enter a bank and hand a note to a teller demanding cash, sometimes claiming to have a weapon and threatening violence should the teller sound the alarm. Banks in the region that will be participating in the policy change include Chase, Fairwinds Credit Union, Fifth Third, Fidelity, Old Florida National, Pinnacle, Wells Fargo, and Trustco. Police said the change would be "just one of several security improvements Longwood banks are implementing and the only one that will be discussed publicly."

IP Theft Costs US $300 Billion Per Year: Report 05/23/13, Voice of America News

A report by the Commission on the Theft of American Intellectual Property (CTAIP) has found that intellectual property theft costs the United States more than $300 billion annually. The commission recommends that the federal government impose economic sanctions against countries where those crimes originate, particularly China, which it says is responsible for 80 percent of all IP theft. Other countries at the top of the list of perpetrators include Russia and India. It also called for import bans and blacklisting from financial markets. The CTAIP additionally said that the president's national security adviser should take the lead on managing the government's response to intellectual property theft. U.S. officials have already taken some diplomatic steps to crack down on hacking against the U.S. government and private businesses to steal trade secrets. Despite this focus on cybersecurity, the commission's report found that intellectual property theft often occurs via stolen equipment, bribery, or pirated software.

Bank Manager Arrested on Suspicion of Theft 06/04/13, Columbian (Washington)

According to Gresham (Ore.) Police Department Detective Brandon Crate, a former bank branch manager at Washington Federal in Vancouver, Wash., was arrested on May 24 after allegedly emptying a dead customer's bank account of $35,000 in October 2012. Pa Houa Vue faces felony charges of aggravated theft, aggravated identity theft, and identity theft, and is being held without bail. According to police, the day before her six-month review at Washington Federal's Gresham branch, Vue told bank employees that she forgot to close a client's account in Vancouver. She allegedly faked a telephone conversation with the client and had the employees cash out the account and write a $35,079.44 check to Hai Lo, which is similar to the name of Vue's husband. Vue then allegedly deposited the check at Clackamas County Bank in Gresham, and is believed to have withdrawn $5,000 in cash and a $13,000 cashier's check at the bank's branch in Boring, Ore., the following day. A co-worker in Vancouver, when tracking down the next of kin for the deceased account holder, found that the account was closed, notified the police, and had a stop payment put on the cashier's check. Crate also discovered the August 2012 disappearance of $12,000 cash from the Vancouver branch's

In The News (cont.)

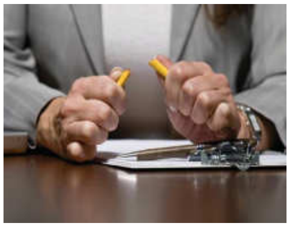
vault, and the November 2011 disappearance of $2,000 from Bank of the West in Southeast Portland. Vue was the manager of that Bank of the West branch at the time the money disappeared.

Maryland Company Cited for Workplace Violence Hazards after Stabbing
06/11/13, Occupational Health & Safety

Maryland's Integra Health Management has been cited by the Occupational Safety and Health Administration (OSHA) for workplace violence hazards following the December 2012 stabbing of an employee by a patient during a required face-to-face hospitalization risk assessment at the patient's home. The citation stated that the company exposed the employee to incidents of violent behavior that lead to that employee's death. Teresa Harrison, OSHA's acting regional administrator for the Southeast, said that "This incident could have been prevented if the employer had a comprehensive, written, workplace violence prevention program to address hazards and assist employees when they raise concerns about their safety." The patient in question had a history of violence, and the employee had raised concerns about that patient prior to the incident.

Companies Say Mexico Security Situation Improving or Steady
Security Magazine (06/13)

Most domestic and foreign firms in Mexico say security has improved or remained unchanged from last year, according to a survey by the American Chamber of Commerce of Mexico. The survey found that 42 percent of the 531 respondents said the security situation had improved. "We attribute this mainly to the actions of the federal authorities and the measures undertaken by the companies themselves," says Thomas Gillen, president of the chamber's security committee. Forty-two percent of respondents said the security situation had not changed while 13 percent said security had deteriorated, of whom more than half cited corruption as the cause of worsening conditions. Nineteen percent of companies surveyed said they anticipated the situation improvising by the end of the year, while 46 percent forecast an improvement within the next five years and 19 percent expect the security situation to remain challenging for more than five years. Extortion has become an issue for more companies, with 36 percent citing the issue this year, compared with 16 percent in 2011. A third of the companies said they had faced security-related losses of up to $1 million, and 4 percent reported losing between $1 million and $5 million. Areas causing the most concern included the northern states of Nuevo Leon and Tamaulipas, followed by the capital, Mexico City, while safer areas included the central state of Queretaro, which has an expanding aerospace and manufacturing sector.



Workplace violence is a complex and widespread issue.

"Maryland Company Cited for Workplace Violence Hazards"

Mexico's security situation improving or remaining steady.

Cyber Security News

Criminals Target the Data Merchants Hold.

“Chinese Hackers Resume Attacks on U.S. Targets”

- New York Times

Effective Threat Defense Requires Clear Security Focus
05/02/13, SC Magazine (UK)

Organizations recognize that security risks are acute, but they typically fail to have a consistent strategic focus. Recent research indicates a need for a dual focus and aligning physical and technology security initiatives. For example, Verizon's 2012 data breach investigations report revealed that 10 percent of breaches involve some form of physical attack, while a further 5 percent result from "privilege misuse." Physical tampering was cited as the second most dangerous threat action used in single-action breaches, following the "exploitation of default or guessable credentials." Other surveys have produced similar findings, such as the physical theft of computers by outsiders. Organizations ideally should merge cyber security risks with improved physical security management. At the same time, there needs to be greater interaction between IT security and physical security teams. Both teams need to acknowledge that cyber attacks may expose failings in the physical security of the premises, and that increased cyber risk may require more restricted physical access to certain areas of the building and office equipment. Any investigation into physical or cyber breaches needs to involve both IT and physical security experts, and the integrated security approach should be monitored by individuals at middle-management.

Criminals Target the Data Merchants Hold
05/09/13, Internet Retailer

Nearly a quarter of 621 data breaches reported in 2012 targeted multichannel merchants and restaurants, according to a new report from Verizon Enterprise Solutions. Only breaches at financial organizations topped those at retailers and restaurants mainly due to the rampant exploitation of ATMs. But retailers accounted for the biggest portion of data exposed via network intrusions at 21.7 percent, Verizon notes. Verizon analyst Suzanne Widup says criminals frequently attack store point-of-sale systems as a way to either infiltrate a merchant's computer network or to steal account data at the store checkout counter. Some retailers implementing Web-based POS systems have spurred criminals to pursue infiltration strategies. “Anything that has an IP address is a target,” Widup notes. Verizon advises retailers to make sure that POS networks, as well as all company computer networks and wireless networks, are routinely patched with updated security software. The Verizon study says payment card account data was most commonly targeted in breaches, followed by personal credentials such as user names and passwords. Criminals “favor payment and personal information that can easily be converted into cash,” the report says.

Chinese Hackers Resume Attacks on U.S. Targets
05/20/13, New York Times

The report the cybersecurity firm Mandiant issued in February about Chinese hacks of U.S. companies and government agencies resulted in a brief lull in those attacks, though security experts and federal officials say that slowdown has since ended. Immediately after Mandiant released its report, hackers who worked for the People's Liberation Army's cyberunit took steps to hide, including removing the spying tools from the systems they had broken into and shutting down command and control servers. But about a month later, the hackers began to gradually start carrying out attacks again, often against the same organizations that they had targeted before, Mandiant says. The company noted that the hackers reinstalled many of the tools that allowed them to surreptitiously steal data and also broke into the computer systems of small Internet service providers and small businesses and used these systems to carry out new attacks. Mandiant says that the hackers are now operating at 60 percent to 70 percent of the level they were working at before its report was released in February. It remains unclear which companies have been targeted in this latest round of attacks, though Mandiant says that many of the victims have been attacked by the Chinese before. These companies include Coca-Cola, Schneider Electric, and Lockheed Martin, though none of them would say whether or not they had been attacked again.

Cyber Security News (cont.)

Former CIA Director Warns About Cyber Threats From North Korea
05/21/13, Wall Street Journal

Former CIA Director R. James Woolsey testified before the House of Representatives Energy and Commerce Committee Hearing on May 21 on cyber threats and security solutions, saying that the country was at risk of being hit with a particular type of cyber attack by North Korea. The attack would use the detonation of a nuclear weapon approximately 30 kilometers above the U.S. mainland to release electromagnetic radiation that could devastate 70 percent of the electric grid and cripple the nation's defenses. He also warned that Iran would soon be capable of launching an electromagnetic pulse attack. Woolsey recommended that the government set standards for the implementation of Faraday Cages, which can shield transformers and other equipment from electrical fields. Others believe that that traditional cyber threats are of greater concern, as the chances of the type of attack described by Woolsey are low. James A. Lewis, the director and senior fellow for the technology and public policy program at the Center for Strategic and International Studies, noted that electromagnetic pulse attacks are "a threat that people have worried about for literally decades without any evidence that it has any basis in fact." Though he acknowledged that it is technically possible that this type of attack would negatively impact the electric grid, he does not believe that a nation possessing only a few nuclear weapons would use on on an attack that may not succeed. Lewis maintains that the biggest cyber concern is coming from Iran, as malicious hackers linked to that country are thought to be behind several sophistical distributed denial-of-service attacks against U.S. financial institutions.

Microsoft, FBI Go After Major Bank Account Stealing Cybercrime Ring
06/05/13, Reuters

Microsoft and the FBI, aided by authorities in more than 80 countries, have launched a major assault on one of the world's biggest cybercrime rings, believed to have stolen more than $500 million from bank accounts over the past 18 months. Microsoft said its Digital Crimes Unit on Wednesday successfully took down at least 1,000 of an estimated 1,400 malicious computer networks known as the Citadel Botnets. Citadel infected as many as 5 million PCs around the world and, according to Microsoft, was used to steal from dozens of financial institutions, including American Express, Bank of America, Citigroup, PayPal, JPMorgan Chase and Wells Fargo.

Former CIA Director Warns About Cyber Threats From North Korea

- Wall Street Journal

Politically Correct Virus: Doesn't refer to itself as a virus - instead, refers to itself as an "electronic microorganism."

- Mark Kaye

BANKING & FINANCIAL SERVICES COUNCIL MEMBERS

Charles Andrews
First Data Corp.

Steve Braden, CPP
Capital One Financial

Larry Brown
First Citizens Bank & Trust

Stephanie Clark, CFSSP
Key Bank

Clark Cummings, CPP
First Bank

Scott Derby
State Street Corp.

Roy Harness, CPP
Fiserv

Terry Huskey, CPP, CFSSP
Wells Fargo

Brian Ishikawa, CPP, CFSSP
Bank of Hawaii

Doug Johnson
American Bankers Association

Richard Lava
Citigroup

Paul Maihi, CFE
Westpac Banking Corporation

Mike Neugebauer, CPP
Fifth Third Bank

James Power, CPP
TD Bank

Gary Reynolds, CFE
Union Bank of California

Steve Ryker, CPP
Wells Fargo

Jim Smith
Bank of America

Kevin Smith, CPP
Sallie Mae, Inc.

Hector Torres, CPP, CFE
Banco Popular

Omar Valdemar, CPP
City National Bank

2013 ASIS Banking & Financial Services Council
Pre-Conference Workshop

A quick glance at the agenda for our pre-seminar workshop in Chicago:

0830-0900	***Welcome & Introductions (Alex Hilton, Brian Ishikawa)***
0900-0950	***"Information Sharing Overview and DDoS Briefing Denise Anderson – Vice President, Government and Cross-Sector Programs, FS-ISAC Chair National Council of ISACs***
1000-1050	***"Crisis Management" Chris Terzik – Vice President, Incident Management & Head of the Incident Management Team - Wells Fargo***
1100-1150	***"Security and Fraud Program, Assessment and Development Strategies" Rick Mercuri, C.P.P.***
1200-1300	***Lunch (hosted by ASIS)***
1330-1500	***"Branch Physical Security" D. Mark Lowers, CFE, President & CEO, Lowers & Associates***
1515-1615	***"Violent Crimes affecting the Financial Services Industry" SA Garrett Croon, & SSA Mark Quinn - FBI Chicago***
1615-1645	***"Active Shooter" – Preparation, Training & Response Rob Shuster, VP Protective Services and Training, AFIMAC***
1645-1715	**"Panel Discussion" (Workplace Violence, Active Shoot er) TBC - Terry Huskey, Hector Torres, Larry Brown**
1715-1800	***Networking session (hosted by Diebold)***

Reminder - If you are attending this year's seminar & exhibits but have not yet registered for our pre-seminar session, please do so as soon as possible.

Banking & Financial Services Council Advisory Members

Brian R. Abraham, CPP 3SI Security Systems	Alexander Hilton, CPP 3SI Security Systems	Steve Longo CAP Index, Inc.