Issue #31
July 2015

GREAT AMERICAN and LOWERS & ASSOCIATES

Fidelity / Crime Observer

Local Library Loses More Than Late Fees

It cannot be stated strongly enough that separation of accounting duties is one of the most important ways to avert employee theft. Yet time and again, companies and organizations fall victim to fraud because they do not have adequate controls in place. One library lost over $1M due to lack of oversight of its accounting officer.

The thefts came to light when the board replaced its director. A board member met with a bank representative to change the authorized signatures on their account. While doing so, the banker mentioned that the accounting officer had recently come in to discuss the two remaining Certificates of Deposit. The board member questioned why there were only two CDs remaining when there should have been four. He was shocked to learn that the accounting officer had previously liquidated two of the original CDs. This triggered an investigation that disclosed additional thefts going back seven years.

The library was on a tight budget and staffing was lean. They had only one employee in the accounting department, the accounting officer, and she reported to the director. On the surface, the accounting officer did a wonderful job maintaining the books of the library. Her responsibilities included depositing receipts, processing payments and payroll, maintaining the general ledger, and reconciling the bank statement. Her scheme included paying personal credit card obligations, cashing petty cash checks, ATM withdrawals, ACH transfers to her account, and of course, liquidating the Certificates of Deposit.

Checks written on the library's account had a dual signature requirement. The accounting officer was one, the director was the other. The accounting officer prepared the checks for payment and obtained the second signature of the director. Unfortunately for the library, the director conducted no review of the payments before signing the checks. The accounting officer also obtained an ATM debit card and made unauthorized withdrawals of cash as needed. As for the CDs, the bank perceived the accounting officer as the contact person on the account. They simply followed her liquidation instructions.

Clearly having one employee control receipts, payments, payroll, the general ledger, and bank reconciliations was the major reason the scheme lasted as long as it did. Because the accounting officer controlled the ledger, she had the ability to cover the thefts by booking the fraudulent transactions to various expense codes. She also was the one that reconciled the bank statement. No one else saw the payments to her credit card company or the numerous ATM withdrawals.

Consolidation of key accounting functions plus a hands-off director was the perfect storm for this fraud, one that lasted for seven years and cost the library $1,000,000.

By Richard A. Searcy, Director, Crime Claims
Great American Insurance Group
Fidelity / Crime Division

Contact List

Great American Insurance Group

Dennis Burns, VP
Fidelity / Crime Division
212.513.4017
dburns@GAIC.com

Lowers Risk Group

Steve Yesko, ARM
Director, Business Development
540.338.7151
syesko@lowersriskgroup.com

Inside This Issue

Whitepaper—
Social Engineering Fraud:
Loss Prevention & Control Guidelines

The following excerpts are from the whitepaper recently published by Lowers Risk Group entitled *Social Engineering Fraud: Loss Prevention & Control Guidelines.* Casino, gaming, and resort operations are not exempt from social engineering fraud scams. Take the best defense against social engineering fraud by understanding its methodology and developing a comprehensive security policy. This white paper covers the fundamentals of social engineering and provides the necessary tools for preventing loss within any organization.

****

Background

In the context of information security, human-based Social Engineering, otherwise known as "human hacking" is defined as the art of influencing people to disclose information and to get them to act inappropriately. Some criminals consider it much easier to abuse a person's trust than to use technical means to hack into a secured computer system, mostly because they have learned how to coerce their targets into giving them information by exploiting certain qualities in human nature. To do this, they use various forms of communication such as email, the Internet, the telephone, and even face-to-face interactions, to perpetrate their scheme of defrauding and infiltrating companies. Social Engineering attacks can take many forms such as being both human and computer-based; however, security experts have recognized that most scams follow a four-stage method: Information Gathering, Relationship Development, Exploitation, then Execution.

Some criminals consider it much easier to abuse a person's trust than to use technical means to hack into a secured computer system.

This methodology, along with the tendency for humans to be the "weakest link" in the security chain, creates a vulnerability that can have a serious operational impact. Since Social Engineering is such a real threat in today's workplace, it becomes essential for employees across an entire organization to be educated and trained on how to detect and prevent this type of fraud. There is also a need for companies to develop and implement specific policies (i.e. employee understanding of confidential and sensitive information and how to keep it safe) to prevent and respond to an attack. Companies must be cautious not to focus their efforts and security budgets entirely on defending against technical attacks from hackers and other electronic threats, thereby underestimating, or even entirely overlooking, the weakness posed by the human element.

A plan to mitigate the effect of Social Engineering attacks should be a part of any comprehensive security policy with a component that raises awareness among employees and educates those who are most vulnerable such as new hires, help desk personnel, contractors, executive assistants, human resource personnel, senior managers and executives, as well as information technology (IT) employees who handle technical and physical security.

According to a survey sponsored by Check Point Software Technologies in 2011, nearly half of the global businesses they contacted reported being the victim of one or more Social Engineering attacks that resulted in losses ranging anywhere from $25,000 to $100,000 per occurrence.

Methodology

Social engineers use many different strategies for gathering information from their targets and some of the methodology used includes the tactics listed below:

- **IVR/Phone Phishing (aka Vishing)—**This tactic involves a technical approach using an Interactive Voice Response (IVR) system to replicate a legitimate sounding message appearing to come from a bank or other financial institution directing the recipient to respond in order to "verify" confidential information.

Continued on Page 3

Whitepaper—
Social Engineering Fraud:
Loss Prevention & Control Guidelines

Continued from Page 2

- **Impersonation/Pretexting**—A common form of deception may involve an attacker using a believable reason to impersonate an authority, pretend to be a fellow employee, IT representative, or vendor in order to gather confidential or other sensitive information.
- **Phishing/Spam/Spearphishing**—Phishing can come in the form of a phone call or email from someone claiming to be in a position of authority asking for confidential information, such as a password. Phishing can also include sending emails to organizational contacts that contain malware designed to compromise computer systems or capture personal or private credentials.
- **SMS Phishing (aka SMSishing)**—This attack occurs when an SMS message is received that is purportedly sent from a reputable source, such as your bank, asking for personal details.
- **Bluesnarfing/Bluejacking**—Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection. Both Bluesnarfing and Bluejacking exploit others' Bluetooth connections without their knowledge. Usually harmless, Bluejacking involves only the transmittal of data to the target device, whereas Bluesnarfing is the theft of information from the target device.
- **Trash Cover/Forensic Recovery**—Attackers collect information from discarded materials like old computer equipment (i.e. hard drives, thumb drives, DVD, and CDs) and company documents that were not disposed of securely.
- **Quid Pro Quo (Give and Take)**—An attacker makes random calls and offers his targets a gift or benefit in exchange for a specific action or piece of information with the goal of rendering some form of assistance so that the victim will feel obligated in some way.
- **Baiting**—A common method used in this type of attack involves leaving a malware-infected device such as a USB drive or CD/DVD at a location where an employee will come across it, and then out of curiosity will plug/load the infected device into their computer.
- **Tailgating/Direct Access**—This type of activity refers to attackers who gain unauthorized access to company premises by following closely behind an employee entering a facility or presenting themselves as someone who has business with the company. In this instance an attacker may state that they left their security credentials inside the facility or at home if challenged by an employee while entering the facility.
- **Diversion Theft**—The methodology in this attack involves misdirecting a courier or transport company; arranging for a package or delivery to be taken to another location.

According to a survey conducted, nearly 50% of the businesses contacted were victims of Social Engineering attacks resulting in losses ranging from $25K to $100K per occurrence.

A plan to mitigate the effect of Social Engineering attacks should be a part of any comprehensive security policy with a component that raises awareness among employees and educates those who are most vulnerable.

Why are Social Engineering Attacks So Successful? How to Recognize and Respond to An Attacker and More.

Select the title to download the complete, free, digital copy of the Social Engineering Fraud: Loss Prevention & Control Guidelines whitepaper. If you have questions about how Lowers Risk Group can assist your organization, we invite you to talk to a risk management consultant.

Great American Insurance
Market Advantage Quick Facts

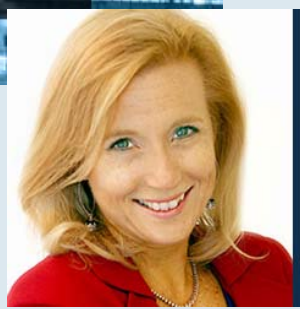
- **The Great American Insurance, Fidelity/Crime Division was established in 1995 and has grown to be the 4th largest crime insurer in the U.S.**
- **A.M. Best rated "A+" (Superior) Class XIII and Standard & Poor's Rated "A+" (Strong).**
- **Great American has had an A.M. Best Rating of "A" (Excellent) or higher for over 100 years.**
- **Licensed in all 50 states and Canada.**
- **$50 million in capacity for Commercial Crime and tailored coverages to meet the specific needs of our clients.**
- **$65 million in capacity for Kidnap, Ransom, & Extortion coverage. $0 deductible applies.**
- **7 regional offices in 3 countries.**
- **Partnership with highly-regarded global risk mitigation firm.**
- **Experienced claim staff only handling Fidelity/Crime claims.**

For more information please visit our website at www.crimeinsurance.com | Applications | Brochures.

Join Us For The 3rd Annual SCTA Conference
September 23-25, 2015
Hyatt Magnificent Mile—Chicago, IL

The conference is designed to support the association's mission to protect, strengthen, and unite the cash-in-transit and cash servicing industries. Attendees benefit from informative sessions, networking opportunities, exhibits, and a keynote address.

Learn more & REGISTER >



2015 Keynote Speaker

Theresa Payton

Former White House CIO, Cybersecurity Authority & Expert on Identity Theft and the Internet of Things.

Read her full bio >