Native American Insider

Issue #21 July 2015

Contact List

Through the transfer of knowledge to you, the tribal government, or enterprise, Tribal First enables you to increase your self-sufficiency in all aspects of risk management. For more information, contact:

Robert Shearer
Senior Vice President
(800) 552-8921
rshearer@tribalfirst.com

Trust your risk mitigation needs to Lowers Risk Group, an independent, internationally recognized provider of loss prevention, investigation, and enterprise risk management (including human capital risk) services to the Casino & Gaming Industry. For more information, please contact:

Steve Yesko, ARM
Director, Business Development
(540) 338-7151
syesko@lowersriskgroup.com

Great American is prepared to provide the insurance protection your casino needs to guard against fraud, theft, robbery, kidnap and ransom, or computer crime. For more information, please contact:

Stephanie Hoboth
Vice President
(860) 285-0076
smhoboth@gaic.com

Employee Theft

A former human resources manager at Thunder Valley Casino Resort has pleaded guilty to theft from the Indian tribal government. Erika Michele Carlton, 38, of Roseville, entered her plea Thursday in federal court. For five years ending in 2011, Carlton embezzled and stole up to $400,000 in money and property from Thunder Valley, the Lincoln CA casino owned by the United Auburn Indian Community, according to the U.S. Attorney's office in Sacramento. Carlton had access to Thunder Valley credit cards and other funds she could use to buy items for employees. Carlton used Thunder Valley funds to buy raffle prizes that were given out at employee functions, such as Christmas parties. The prizes included gift cards, iPods, and televisions. Prizes were either kept by Carlton or returned to the store for cash or merchandise credit for her own use, according to the press release.

Source: The Sacramento Bee. August 3, 2012

Employee theft can occur at all levels and in all departments of a casino operation. A report by the American Gaming Association affirms that the casino gaming industry supports 1.7 million jobs and is expected to add more than 62,000 by 2024. The dominant types of employee theft include the following:

- ❑ Cash handling positions on the gaming floor in cashiers' cages, back rooms, and Point of Sale terminals
- ❑ Theft of alcohol and food from casino receiving docks

Gaming is a big business, and the product is money. Regulations set by gaming control boards require casinos to establish and present a system of internal controls. This includes accounting procedures, authorized processing, record keeping, safeguarding securities and assets, financial recordings, etc. A significant amount of time and money is put into the research and implementation of these internal controls, but who holds the responsibility of executing them? How much time and effort is put into finding the right people to carry out these duties?

Casinos must put more of an emphasis on their recruiting and hiring practices. A good example of this would be talent assessments. Talent assessments, also called pre-employment tests or employment screening tests, are used to help employers identify candidates that will be a good fit for jobs at their company. Employee screening tools such as this can help to identify potential problem hires before offers of employment are made.

Thorough background checks are essential. When conducting criminal background checks, be sure to go back at least seven (7) years. Jurisdictions where an applicant has previously resided should also be checked. Credit checks are a critical tool when screening potential employees.

Continued on page 4

Inside This Issue

Mitigating Risk for the Casino & Gaming Industry

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.

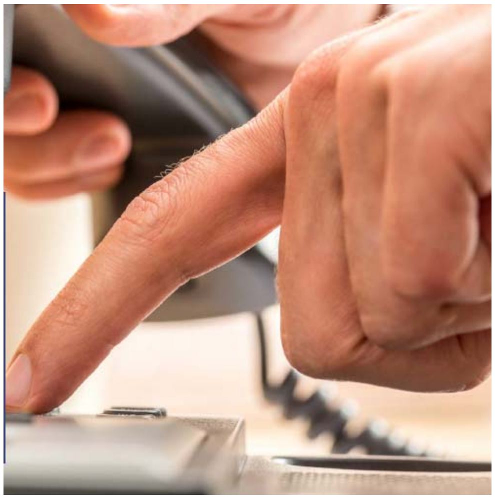
****

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.

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

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.

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.

Employee Theft

Continued from page 1

These reports will show details about an applicant's credit card debt, mortgage, car payment, student loans, as well as late payments and defaulted loans. People with financial difficulties may be more prone to commit fraud. In order to run a credit check, you are legally required to notify the job applicant in writing that a credit report may be requested. The applicant will need to give the casino written authorization and consent. This procedure will also help in the pre-screening phase of hiring.

The additional tips below will also assist you in hiring honest and good employees:

- ❑ Use the **employee's application.** Check and verify everything.
- ❑ **Resume red flags**. Look for gaps in employment. Are there any inconsistencies?
- ❑ **Reference checks**. Request at least one personal reference in addition to a professional one.
- ❑ Be clear with the **job description**. Customize the job description to fit the organization and the skill set necessary. The majority of employers use standard job descriptions that can be found on the internet. The more precise the job description, the better chance you have of receiving quality applicants.
- ❑ Be **proactive**. Seeking employees only when a job needs to be filled can cause pressure to hire someone immediately. In that instance, employers tend to be less selective and a bad hiring decision may be the result.

Investing time and money in your hiring procedures can save your gaming operation from the complications of poor hires. For more information on pre-employment screening, please contact Great American Insurance or Lowers & Associates.

By Tara Proulx, Sr. Acct. Executive
Great American Insurance Group
Fidelity / Crime Division

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.

20th Anniversary
Fidelity/Crime
Protecting businesses since 1995