Native American Insider

Issue #22 October 2015

Contact List

TRIBAL FIRST
INSURING NATIVE AMERICA

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

LowersRiskGroup
Protecting People, Brands, and Profits

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
INSURANCE GROUP

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

Check It Twice

A lack of separation of duties remains one of the leading causes of fidelity losses. Many times, something as simple as a second set of eyes reviewing someone else's work is all that is needed to either prevent a loss or minimize it. An illustration of the importance of internal controls can be seen in this example of a midsized casino in Pennsylvania that allowed their Director of Taxation to have sole authority over all tax related matters.

It all began when a casino owner was informed that something was awry — a tax accountant realized a tax return check issued to the casino was never accounted for. When the tax accountant discovered that the check was deposited into a different account (at the same bank where the casino maintained accounts), she called the bank for details regarding the missing check. Due to privacy concerns, the bank would not reveal who the account belonged to, but confirmed the account was not in the casino's name.

Once it was confirmed that the funds had been deposited into an account not owned by the casino, the CFO got involved. The CFO was eventually able to learn from the bank's branch manager that an employee at the casino presented documentation to the bank indicating he was an authorized signatory on the Insured's accounts, which was not the case. This allowed the employee to set up accounts that the bank believed belonged to the casino, when they were in fact his own personal accounts.

Upon further investigation, the scheme was revealed. The Director of Taxation simply transposed letters within the casino's name or added an additional "o" at the end of "casino" in the Insured's name. When the checks were quickly reviewed, the alterations went unnoticed.

Although the bank should have been more attentive and noticed the discrepancies when handling the checks, better controls by the casino would have helped prevent this type of loss. For most losses, something as simple as having an additional employee reconcile bank accounts or review another's work could have stopped this type of fraud from the very beginning, if not have prevented it altogether. In this case, the Director of Taxation had sole authority to prepare and sign tax refund requests, reconcile the sales tax payable account, and was provided with all tax related checks including payroll, income, and sales tax. This scheme went on for over 6 years, which resulted in a loss of over $1,750,000. In this example, all it took was one employee to notice one missing check for the fraud to be exposed. Ensuring proper segregation of duties helps businesses minimize their chances of loss, saving time and money in the future.

The above narrative is fictional; however, it is based on situations that have been reported.

By Steve Arduini, Account Executive
Great American Insurance Group
Fidelity / Crime Division

Inside This Issue

Hackers Gonna' Hack: Recap of Theresa Payton, Former White House CIO, at the SCTA Conference

October 1, 2015

By: Lowers Risk Group

True or False: 95% of all security breaches are due to sophisticated cybercriminals that we could not defend ourselves against. Believe it or not, the answer is false. In fact, we are most often victims of breaches due to human error which is linked to poor security design.

The recent Secure Cash & Transport Association (SCTA) Conference, which brought more than 200 cash management industry thought leaders to Chicago, was filled with insightful speakers and important discussions about the security, transportation, and management of cash in today's world. Foremost among them, was Keynote Speaker and former White House CIO, Theresa Payton, who stressed the need to design security "for the human psyche." As Ms. Payton so astutely pointed out, 95% or more of past breaches were a result of human error, this according to the 2014 IBM Security Services Cyber Security Intelligence Index. From clicking on a malicious link found in a phishing email, to running servers that are set up with the wrong settings, to lost laptops or portable media, human error is a huge concern.

To illustrate the point, Payton and her team conducted a geofencing test to show how a hacker might target companies through individuals. Similar to how a physical security team for a rock star might draw a circle around a venue and look at all the entrances and exits to the venue to ensure the safety of the rock star and the crowd, in the digital sense, geofencing was used to demonstrate how any of us, while connecting with loved ones through social media, could expose too many clues.

Payton explained the steps of her geofencing experiment, which involved drawing a "digital circle" around a physical location, using tools to see all social media being posted within or near the geofence, reverse facial recognition, geolocation tools, and demonstration of how all of the data collected could be used to trick the subject into giving access to a network of data.

The point of the experiment was to demonstrate why it is so critical that all security programs help design and manage through the human psyche, and not against it.

Designing Security for the Human Psyche: Evolutionary Change Required

Payton stressed the need to design applications under the assumption that your users will do everything wrong – they will share passwords, they will forget them, and they will do unsafe things to get their jobs done, such as use free, unsecure WiFi.

Continued on page 3

Hackers Gonna' Hack: Recap of Theresa Payton, Former White House CIO, at the SCTA Conference

Continued from page 2

To make evolutionary change, Payton suggests we need to incorporate the following scenarios:

- ❑ Understand and educate the knowledge of human nature and psyche into the cyber security profession.
- ❑ Incorporate that knowledge into the design and implementation of all our systems.

Innovate cyber security technologies and policies that account for insecure human behaviors and incentives. Unless we do these things, she contends, our privacy and security will perish.

How can you put these changes into action?

Payton suggests the following five steps:

1. Design security awareness and rules with your end user in mind.
2. Knowing users will break all the rules by accident, segment your most critical data elements away from every day access (different credentials, limited access, expiring passwords).
3. Use expiring and limited credentials. In a recent study, 70% of people polled said they have access they don't really need and many admitted they peak at the data because they have access!
4. Implement "digital shredding." Just like you wouldn't keep overstuffed paper files and cabinets, Payton suggests getting rid of unneeded data in the digital sense.
5. Reward reporting. Make it easy and recognize and reward employees who report malware, strange emails, or other suspicious files or network activity.

The US Director of National Intelligence has ranked cybercrime as the top national security threat, higher than that of terrorism, espionage, and weapons of mass destruction. A threat of this level is bound to impact everyday organizations. Payton made the impactful statement that at some point technology will fail and process is all that will remain. This is why she says it is so very important to design for the human psyche.

Is your organization on the offense when it comes to addressing cybersecurity and the human psyche? We'd like to hear from you.

To Hire An Ex-Offender or Not: Evaluating Your Risks

Should you hire an ex-offender? The easy answer is "it depends," but in the real world you can't just peer into your applicant's eyes and get the answer. The employer's dilemma is that the choice you make exposes you to potential risks of competing types.

The socially-beneficial choice is to hire ex-offenders, and right now there is a lot of pressure on employers to do just that. (Assuming, of course, there are not very legitimate reasons to exclude them based on the risks inherent in the role.) The threads in the conversation on this issue range from feel good stories about employers who have had great successes hiring ex-offenders to organized movements working to get more job opportunities for them. These mostly positive stories are backed up by the legal mandates of employment law rooted in anti-discrimination concepts.

Yet employers are still responsible for the safety of their customers and workers. To the extent that having committed a crime in the past is a predictor of future anti-social actions, ex-offenders seem to pose extra risk. If these risks materialize, the employer is potentially liable for negligent hiring or retention.

A common response to the risks associated with hiring ex-offenders is for employers to adopt a "blanket" exclusion policy and simply reject all applicants who have a criminal history. Unfortunately, neither hiring every ex-offender who walks in the door nor rejecting every one of them is an effective way of managing the competing risks. The better course involves making decisions on individual applicants; taking the relevant factors into account. Read this complete blog and get our free guide below. Proforma Screening Solutions is a Lowers Risk Group company.

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.

Mitigating Risk for the Casino & Gaming Industry