Native American Insider

Issue #16 April 2014

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
VP, 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

Be Cyber Safe: Understanding and Avoiding Cybercrime

Cybercrime is on the rise and organizations and individuals are more aware than ever of the growing epidemic. Unfortunately, many organizations are still not adequately prepared from an insurance perspective. A simple perusal of the media landscape paints a vivid picture of the urgency to protect against cybercrime:

- The Target episode alone is reported by the *New York Daily News* to have affected as many as 70 million Americans (approximately 23% of our population according to the 2010 census).
- The October 24-31, 2011 issue of *National Underwriter Property & Casualty* identifies cyber liability as a top concern in the Lawyers' Professional Liability Market.
- The October 2013 *Norton Report* indicates that while the number of internet users who have been impacted by cybercrime victims has decreased, the average cost per incident has increased by 50%.
- In the same report, a study of 13,000 adults across 24 countries assert that most smartphone users "do not take the basic precautions such as using passwords, having security software, or backing up files from mobile devices," despite the fact that 49% of consumers use their personal mobile devices for both work and play.

So what is cybercrime? It's a lot of things, including phishing/spear phishing, network intrusions (hacks and malware viruses), and rogue employees. Cybercrime can also result from improper disposal of paper and electronic data. A data breach occurs when there is a release or disclosure of information to an unauthorized individual or entity that may cause a person or company financial or reputational damage.

The government is attempting to thwart cybercrime through legislation, but it is difficult to keep in step with something that is constantly evolving. There are a number of federal laws in the United States aimed at protecting the unauthorized release of information, the more familiar ones being HIPAA (Health Insurance Portability and Accountability Act) and FACTA (Fair and Accurate Credit Transactions Act). More than 46 states also have their own laws, which differ based upon trigger notices, timeliness, and required content for notification. International laws also exist such as the European Union Directive relating to cookie consent, safe harbor provisions, and binding corporate rules.

Unfortunately, legislation can only go so far in diminishing the threat of cybercrime. The most important safety measures must occur within the organization. How does one guard against cybercrime? The solution is similar to managing other forms of risk and protecting against perils such as business interruption loss. Start with building cybercrime protection into your crisis management plan and work with legal counsel to ensure a comprehensive process. It has never been more important than now to address cyber liability exposures.

Continued on page 4

Inside This Issue

Taking Advantage of Trust

A well operated human resources department is critical for any business, and casinos are no exception. Considering the diversity of departments within a casino and the unique functions performed by the employees, it is not an easy area to manage. The human resources managers must be highly intelligent and experienced. Unfortunately individuals in these management positions can take advantage of their good reputations and use their position for personal gain that is detrimental to their company.

A small casino in the southwest U.S. opened up in the mid 1990's and within a few years had grown to include several hundred slot machines and approximately thirty table games. The casino grew to a staff of around three hundred employees by early 2000 when they hired a new HR manager who had previous experience working in the gaming industry.

The new HR manager immediately contributed a well-received style of management and organization the department previously lacked. He took it upon himself to get involved in the day-to-day functions and worked with a very hands-on approach. The casino's management was very pleased with his performance and decided to make him responsible for overseeing all aspects of the payroll functions as well.

Like any small to mid-sized business, healthcare insurance and employee benefits are a significant expense to the casino. They chose the most reasonable program they could find and allowed the HR manager to take care of the rest.

During the various forums regarding their benefits package, the HR manager empathized with the employees who felt the costs were high and assured them he paid the same premiums and that it was the best option available. In actuality the latter part was true; it was the best option available, but he was not paying the same price.

One day an employee within his department saw a medical bill with the HR manager's name on it left on the copy machine tray. She decided to flip it upside down and delivered it to his office so that his personal information would not be left out in the open. While she thought this was a kind gesture, the HR manager uncharacteristically ranted about how she was out of place for picking up his private material. It seemed very suspicious to her and she decided to report the incident through their anonymous hotline.

Around this time, the HR manager took a three week vacation leaving someone else temporarily in charge of the payroll and benefits administration. While performing the payroll duties, the employee noticed names of individuals that no longer worked for the casino were still listed.

It was the perfect storm. A full audit and investigation was launched and the HR manager's fraudulent activity was revealed. The HR manager had the most comprehensive health and life insurance coverage option, but was paying for the least comprehensive. On top of that, the coverage was extended to his wife without additional premium.

Since he had found it easy to gain this coverage without detection, he had broadened his theft. He took advantage of overseeing the payroll by performing various ghost payroll schemes throughout the year. Individuals who were no longer employed were being kept on the payroll for several months after their termination or resignation. He manipulated their paychecks and diverted them to his bank account.

The scheme lasted nearly 10 years and the misappropriation of funds totaled close to $500,000. The casino management has since instituted a separation of duties between the payroll and human resources functions. Additionally, both departments now have more oversight from senior management. Specifically regarding the payroll duties, persons who are authorized to hire/fire employees no longer distribute the payroll. The casino management now has a respect for these procedures. They have come to the unfortunate realization that even exceptional employees should not be trusted to have excessive authority with no oversight.

By Patrick Shannon, Sr. Acct. Executive
Great American Insurance Group
Fidelity / Crime Division

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

How You Can Cut Your Organization's Risk Of Fraud by 50%

You've seen the data before: Organizational fraud is a huge annual cost. Managers want to reduce the costs, so the real questions are to learn why fraud occurs and what to do about it.

The most compelling explanation for organizational fraud is the Fraud Triangle. Frauds occur when there is opportunity, one or more employees are under perceived financial pressure (incentives exist), and they can rationalize their fraudulent behavior. These three factors correspond to the legs of the Fraud Triangle.

1. Control the Opportunities to Reduce the Chances of Fraud

In our experience, organizations can reduce the probability of organizational fraud by just removing one of the legs of the triangle. There are things you can't control, such as employees' spending habits, but if you remove the opportunity for employees to get their hands on an asset without the potential of getting caught, then you've reduced that probability by 50 percent.

2. Opportunities for Fraud Can Emerge as Unintended Consequences

Some of the factors that can promote opportunities for fraud can be linked to cost reducing strategies since modern businesses try to run very lean. In other words, these opportunities become unintended consequences of well-motivated management decisions.

For instance, coupled with technology, companies can turn more complex processes over to one or a few people, reducing the number of controls required to protect precious assets. For example, in a situation where a single person can balance accounts, and write and sign checks, an opportunity is created. At the same time, managers have fewer avenues for personal oversight of complex organizational structure; they may even cut back on the frequency and depth of internal or external audits.

3. Tactics for Thwarting Fraud

Taking steps to reduce fraud not only saves an organization money directly, it also addresses the underwriting criteria insurance companies are likely to use in evaluating a company. Some of the tactics you can use to prevent and detect fraud, as well as demonstrate the security of your program to the insurance companies, include:

- ☑ Internal controls
- ☑ Segregation of duties
- ☑ Comprehensive employee background screening
- ☑ Vendor screening and due diligence
- ☑ Establishment of a tip line or whistleblower program
- ☑ Set the "Tone At the Top"

Controlling organizational fraud requires management review and an organizational culture that promotes healthy behavior. Removing the opportunities for fraud is a vital first step, but one that needs to be revisited on a regular basis as the organization evolves. The opportunities you are trying to suppress are often the unintended consequences of actions you take to grow your business.

By Mark Lowers
President
Lowers Risk Group

Be Cyber Safe: Understanding and Avoiding Cybercrime

Continued from page 1

Management should establish policies and systematic processes in order to encourage sustainable cyber risk reduction and prevent harmful attacks. The following are six steps that will help accomplish cyber risk reduction objectives:

1. **Password Security:** Systems should prompt regular password changes and disallow repetitive use of previous passwords. As a best practice, experts recommend a practice of changing passwords at least every other month.

2. **IT Software and Security Strategy:** IT should routinely update anti-virus software and refrain from accessing confidential data over unsecured and/or public wireless networks.

3. **Designated Computer for Banking:** It is more difficult for outsiders to access important records by using a single computer for online financial transactions. The machine should not be used for email, web-surfing, or social media, which can be conduits for hackers.

4. **Duplication:** Take advantage of developments in cloud computing to restore systems in the event that networks are manipulated.

5. **Educate. Educate. Educate:** IT personnel aren't the only ones tasked to be on the lookout for cyber attacks. Employees need to be trained to recognize and report suspicious activity.

6. **Get Insured:** Sometimes despite best efforts, another line of defense, such as insurance, is still necessary. Also, consider how your organization will go about repairing a damaged reputation in the event a breach occurs.

By Randall Sachtler, CSP, Sr. Risk Control Consultant
Alliant Insurance Services

NEWS: Should Patron Have To Pay $500,000 Casino Debt?

March 7, 2014 — A man who lost $500,000 gambling during Super Bowl weekend in Las Vegas is suing the casino claiming he shouldn't have to pay the debt because he was over-served and allowed to gamble. Mark Johnston's attorney, Sean Lyttle, stated that his client was staying at the Downtown Grand, and the establishment began serving his client alcohol as soon as he landed in Las Vegas.

From what they've come up with so far, Lyttle says it appears Johnston gambled for around 17 hours uninterrupted during which time he was served anywhere from 25 to 30 additional alcoholic beverages and was issued markers totaling $500,000, which could be a problem for the casino.

"The basis of our lawsuit is that Nevada gaming regulations prohibit a casino, a gaming licensee, from serving complimentary alcoholic beverages to someone who is visibly intoxicated, and the regulations also prohibit casinos from dealing cards, or allowing a patron who is visibly intoxicated to gamble," says Lyttle.

"In this instance, the Downtown Grand not only served Mr. Johnston comped drinks and dealt him cards while he was visibly intoxicated, but they also issued him half a million dollars in markers during this period of time that he was visibly intoxicated."

By Michael Martinez & Kyung Lah
CNN Cable News Network