GREAT AMERICAN and LOWERS RISK GROUP

Issue #35

July 2014

The Casino Shield

Think Theft Can't Happen At Your Casino? Think Again!!!

Below are actual news headlines, all associated with losses in the gaming industry:

"Former Casino HR Manager in California Pleads Guilty to Embezzling $400K"

"Virginia Women Charged with Embezzling more than $1.2 Million from a Casino & Racetrack"

"Police Arrest One, Search for Another after Casino Robbery and Chase"

"Mississippi Woman Accused of Embezzling $195K from Casino"

"Alabama Women Sentenced in Casino Embezzlement Case"

"Suspects Arrested in String of Convenience Store, Casino Thefts"

"New York Couple Sentenced in Embezzlement Casino Laundering Case"

"Iowa Woman Sentenced to 15 Months Prison for Casino Embezzlement"

"Former Woodstock Woman Pleads Guilty in Casino Nightclub Embezzlement Scheme"

"Atlantic City 'Fake' FBI Agent Convicted of Casino-Hotel Robbery"

To keep your casino out of the headlines, here are some internal controls to consider:

- ❑ Ensure adequate barriers are placed between the cashier's cage and the patrons. Steel bars are recommended.
- ❑ Armored car service should be used for all deliveries of money, securities, and other valuables.
- ❑ Limit cash on hand by scheduling frequent deposits.
- ❑ Implement an authorized master vendor list and conduct background checks on all vendors. Vendor Fraud is the number one type of employee theft loss.
- ❑ Establish or review the casino's employment screening program consisting of background checks and drug tests, and ensure the program is comprehensive, role-specific, and legally compliant.
- ❑ An annual CPA audit is recommended.
- ❑ Proper segregation of banking and payroll duties is crucial.

Source: http://fraudtalk.blogspot.com/

By Tory Knauf, Account Manager
Great American Insurance Group
Fidelity / Crime Division

Contact List

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 M. Hoboth
Vice President
(860) 285-0076
smhoboth@GAIC.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
VP, Business Development
(540) 338-7151
syesko@lowersriskgroup.com

Inside This Issue

Mitigating Risk for the Casino & Gaming Industry

Are You Doing Enough To Protect Against Financial Fraud?

Yet more evidence of the prevalence of financial fraud against organizations has emerged from a recent poll by Kyriba. The poll found that almost 80% of organizations had been victims of fraud. The very high proportion of victims is startling in itself, but it is consistent with information we have presented in previous articles that organizational fraud is a global problem, costing 5% of top line revenue annually.

Almost 30% of the respondents to the Kyriba poll reported suffering financial losses, but we think this is a conservative number in this context. Organizational fraud is a hidden crime that sometimes is difficult to detect, even long after the fact. When organizations do detect fraud, they may have incentives to minimize publicity about the crime, so underreporting is probable.

Fraud Occurs, But Fraud Prevention Lags

Taken together, this information is a clarion call to executives and managers to implement rigorous anti-fraud controls. Yet the poll found that over one-third of respondents had not reviewed or updated their fraud prevention controls in over a year. In fact, 18% believed that their organization had *never* installed or updated a fraud prevention program.

Sometimes it seems like it should be easier for victims, many of whom are sophisticated individuals or organizations, to detect financial fraud. But the Bernie Madoff case has shown us how easily investors can be fooled by timing deposits, moving cash from one account to another, delaying responses to questions, or simply not providing requested information at all. All of these kinds of subterfuges should be detected by a fraud prevention program, but obviously the program has to exist in the first place.

A new range of threats has evolved in the rapid growth of extensively networked digital systems. We have seen the massive losses that external theft can cause, as in the Target case, but loss potential is also large for internal theft and fraud. The challenges in these cyber thefts involve both organization (comprehensive access control, for example) and continuous reviews of performance through audits of digital transactions.

Active Prevention Processes are Essential

We have long argued that systematic financial fraud prevention controls should be an integral part of every organization's risk management program. We cannot know with certainty, in advance, when unseen flaws in controls will be found, or flaws in software will come to light.

An organization's best defense against these possibilities is regular, rigorous audits and internal controls designed to detect irregularities in financial flows quickly.

By D. Mark Lowers, CEO
President / CEO
Lowers Risk Group

How Are You Handling This Year's Emerging Risks?

The Edward Snowden case and the theft of Target customer data have both driven home the point that cybersecurity is an emerging, and rising, risk issue for both companies and political entities. But there are other risks that emerge as rapidly-changing multi-market regulatory and business interactions redefine the landscape.

Every year business consultant CEB (Corporate Executive Board) issues a list of emerging risks that sharp companies need to address to stay ahead of the game. This year they recommend managers pay special attention to these 10 specific risks:

1. Compliance management
2. Cybersecurity: malicious insiders
3. Risk management
4. Cybersecurity: malicious outsiders
5. Emerging markets
6. IT governance
7. Third-party relationships
8. Project management
9. Intellectual property
10. Crisis response management

The main reason to review a list like this is that changes in the business environment can make companies' risk management plans obsolete or improperly targeted. Changes in regulation alone make compliance a major problem, not to mention the fact that multiple regulators issuing new rules may create unintended conflict that in turn increases the potential for compliance risk. Risk managers need to allocate resources to evaluate and respond to this new control environment.

An Actionable Emerging Risk Agenda

To help move you toward an actionable plan to address these emerging elements, Friso Van Der Oord and Jeffery Ugbah at RM magazine have consolidated the 10 risks identified by CEB into four analytical themes. The themes are:

The downside of business interdependence: Businesses are increasingly entangled in networks of stakeholders, partners, clients, and suppliers who expose them to risks that are difficult to identify and evaluate.

Balancing business control and value creation: The risks of many new business opportunities are opaque, such as in emerging markets. In these circumstances, managers have to make difficult decisions balancing risk against expected value.

Embedding compliance and risk discipline into the business: The increasingly complicated and sometimes conflicting regulatory demands require a higher and more sophisticated approach to compliance management. Formal full-scale enterprise risk management initiatives are part of the solution.

Continued on page 4

How Are You Handling This Year's Emerging Risks?

Continued from page 3

Blind spots inside our organizational perimeter: Dependence on digital technology creates new risks within the organization, as well as in the external networks it is connected to. IT security spanning everything from cyber spying to employee fraud becomes even more urgent.

The speed of change is not likely to slow down anytime soon. It will continue through good economic conditions and bad as governments, corporations, and businesses in general seek to gain advantages and control. Smart organizations will commit significant resources to identify these tendencies and develop policies to cope.

If you need help formulating your enterprise risk management strategy, let's talk.

By D. Mark Lowers, CEO
President / CEO
Lowers Risk Group

The Value of a Quality Employment Background Check

Since 9/11, the number of background checks performed on job applicants and employees has ballooned, for reasons ranging from heightened security concerns to legal mandates to conduct background checks. Coinciding with this, the amount of digital information available about individuals has increased many times over, and the Internet has given us easier access to it.

In these circumstances, it is easy to understand why employers might want to try tapping into that big pool of online information themselves, or through "instant" background checks. However, there are some very compelling reasons why quality background checks performed by a professional background screening company can offer you a better value and greater protection for your time and money:

1. Helps employers find "good hires" who will improve the organization.
2. Mitigates the risks of a "bad hire".
3. Ensures compliance with the Fair Credit Reporting Act (FCRA)
4. Provides an affirmative legal defense against claims of negligence.
5. Avoids discriminatory practices.
6. Improves compliance with federal, state, and local mandates.
7. Avoids the perils of do-it-yourself online background checks.

To view this article in its entirety, please visit http://www.proformascreening.com/blog/2014/06/19/quality-background-check/.

By Michael Gaul
Vice President, Marketing
Proforma Screening Solutions