GREAT AMERICAN & LOWERS RISK GROUP | ISSUE #40 | JANUARY 2018

FIDELITY/ CRIME OBSERVER

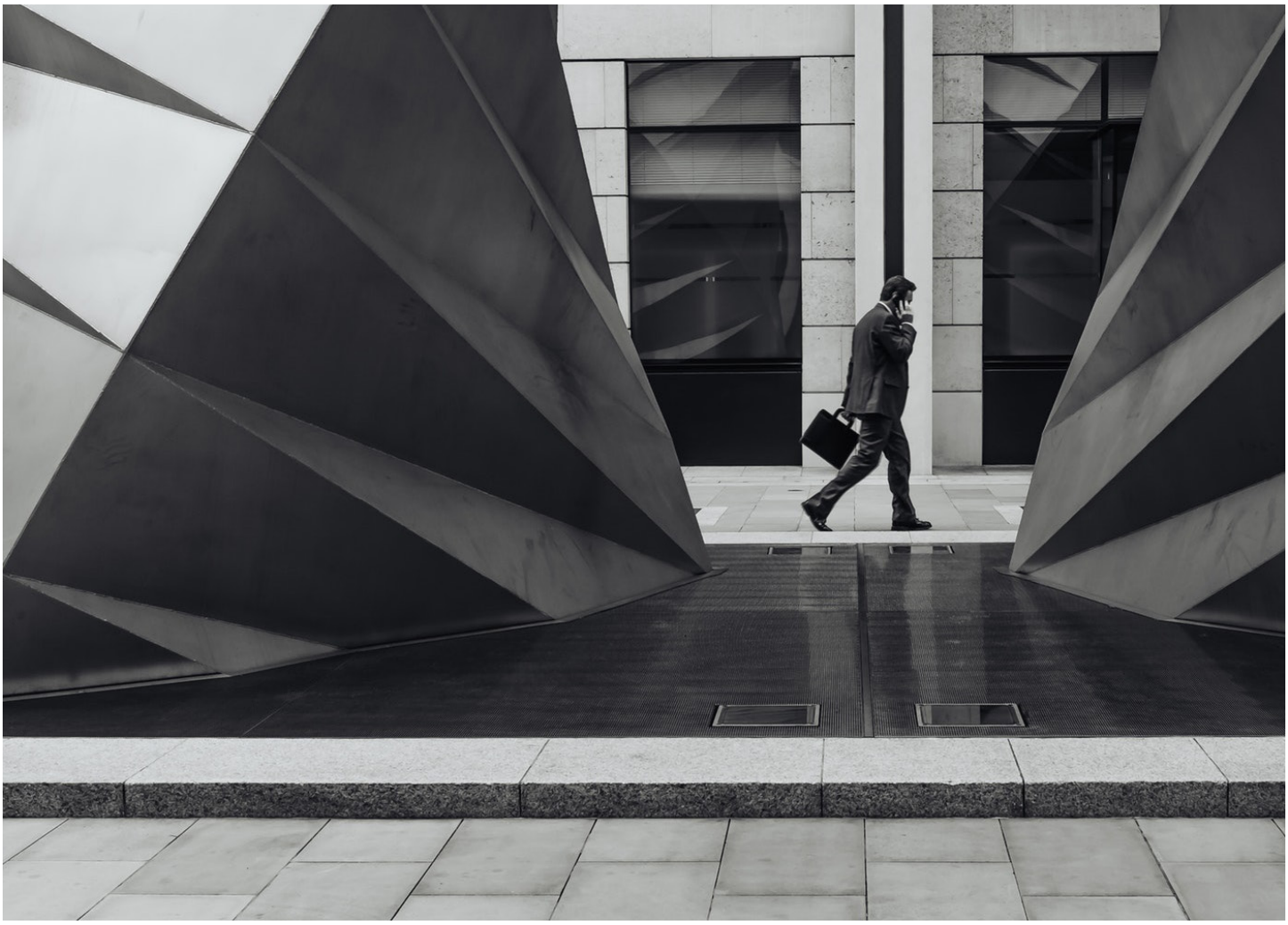

TABLE OF CONTENTS

WHY NOW IS A GREAT TIME FOR A FRAUD PREVENTION CHECK-UP

The ending of one year and beginning of a new year is a great time to give your organization a fraud prevention check-up. This natural time of reflection and renewal provides an opportunity to better protect your organization from the risks of fraud.

The Association of Certified Fraud Examiners (ACFE) suggests that a fraud check-up can save your company from disaster. Wondering how? Consider that fraud can be catastrophic, some can even put you out of business overnight. Even if survived, a major fraud can damage your company's reputation so severely that it can be difficult, if not impossible, to recover. Performing a fraud check-up can help you pinpoint opportunities to rid your organization of fraud. It can expose your company's vulnerabilities and allow you to take a more proactive approach to risk management.

If you're still questioning the importance of a fraud check-up, consider the 18 fraud facts highlighted in our latest slideshow, which come from the ACFE's *Report to the Nations on Occupational Fraud and Abuse* on page 3 of this newsletter.

View our latest blog here: http://blog.lowersrisk.com/fraud-prevention-checkup/

ABOUT US

Lowers Risk Group
provides comprehensive enterprise risk management solutions to organizations operating in high-risk, highly-regulated environments and organizations that value risk mitigation.

Great American Insurance Group
understands the importance of choosing a financially strong company. We are an organization built for the long term and are committed to giving you that strength. For nearly 150 years, Americans have trusted us to protect them. Our innovative insurance solutions and specialization serves niche marketplaces that we know well. This expertise gives us a successful foundation that spans generations.

CONTACT

GREAT AMERICAN INSURANCE GROUP

Dennis Burns, SVP
Fidelity / Crime Division
212.513.4017
dburns@GAIG.com
greatamericaninsurancegroup.com

LowersRiskGroup®
Protecting People, Brands, and Profits

Brad Moody
EVP Operations
540.338.7151
bmoody@lowersriskgroup.com
lowersriskgroup.com

18 FRAUD FACTS

Drive Your 2018 Fraud Prevention Plan

Every two years, the Association of Certified Fraud Examiners (ACFE) performs and publishes research on worldwide organizational fraud.

INCIDENCE. CHARACTERISTICS. IMPACT.

These reports provide a bedrock data-based description of the incidence, characteristics, and impact of fraud on organizations of all types.

Here are 18 facts straight from the report that can help you understand and respond to the threat of organizational fraud in your organization.

1. Organizations worldwide lose about 5% of top-line revenue to organizational fraud.
2. In 2016, the total loss to fraud was estimated at $6.3 Billion, an average loss of $2.7 Million.
3. The largest median losses were in companies exposed to the market, whether privately held or publicly traded, at about $180,000 per case.
4. Median loss due to manager/executive fraud: $703,000 compared to a median loss of $65,000 due to frauds caused by employees.
5. Active detection methods such as controls or surveillance were much more effective in finding frauds.
6. Financial statement fraud, was the least common form of fraud at 10% of cases, but it resulted in a median loss of $975,000.
7. The median loss of small companies was as large as that of large companies, but, predictably, the impact was much larger. By contrast, the more common threat of asset misappropriation at 83% of cases caused a median loss of $125,000.
8. Frauds that lasted five or more years caused median losses of $850,000.
9. 94.5% Of perpetrators attempted to conceal their crime usually by altering documents that may have been evidence.
10. 1% Of discovered frauds were found due to a tip but organizations with hotlines received many more tips than those without (47.3% V. 28.2%).
11. Whistleblowers are more likely to report to supervisors or executives using online methods more than direct contact.
12. Type of fraud varied: small organizations were more likely to experience opportunistic crimes like skimming, while large ones were hurt by corruption.
13. 82% Of organizations had implemented external audits.
14. Small organizations were less likely to have anti-fraud controls in place.
15. Organizations with anti-fraud controls in place had fewer frauds and were able to detect frauds more quickly.
16. Occupational frauds tend to be committed by first-time offenders. Only about 14% of fraudsters had a record of fraud or were fired for fraud-related activity.
17. 8.4% Of victim organizations were fined.
18. In 40.7% Of cases, the victim organizations decided not to refer their fraud cases to law enforcement, with fear of bad publicity being the most-cited reason.

EVERY ORGANIZATION IS AT RISK OF FRAUD.

Lower your risk with the right approach.

We invite you to request a conversation with a Lowers & Associates Certified Fraud Examiner.

NO ONE WANTS TO QUESTION THE BOSS

By: Timothy Marley, Assistant Vice President Great American Insurance Group, Fidelity/ Crime Division

The Jones family owns and operates a fishing equipment manufacturing business that supplies their products to various retailers throughout the Pacific Northwest. The executive team of the company is comprised of company founder Steve and his 3 adult sons Mike, Robbie and Chip. Steve has taken a less active role in the company lately, preferring to spend his time fishing instead of making and selling lures. Regardless, he has check signing authority for all company business. The day to day business of the company is run by oldest son, Mike. Mike has a reputation among their 50 employees for being somewhat of a tyrant of a boss, running the company with a heavy hand. Even Robbie and Chip are somewhat fearful of him.

Mike was out of the office on vacation. But he is known for having a tough time relaxing – often working while away on personal time. During this vacation, someone impersonating Mike contacted an accounting manager at their Seattle WA office via e-mail initially requesting that she process wire transfer payments to a vendor. The request seemed legitimate because first, the vendor was a supplier who was known to both the accounting manager and Steve and second, it was not unusual for Mike to work on business even while on vacation. Through continued e-mail dialogue between the imposter and the accounting manager, the manager agreed to issue two wire transfers. Accordingly, the first one was completed on September 9, 2017 in the amount of ***$650,500 and the second one on October 14, 2017 in the amount of $550,780.***

The loss was discovered when the legitimate vendor needed to be paid and it came to light that Mike never requested the payments previously sent. Unfortunately, funds were quickly transferred to an overseas bank and could not be recovered.

Executive impersonation is a type of scheme known as social engineering that is one of the latest methods used by criminals to induce unsuspecting employees to transfer funds to the fraudsters' bank accounts. Often times an impostor posing as an executive will use "time is of the essence" or "this must be kept confidential" when making the request.

Similar schemes involve a fraudster posing as vendors. The fraudster may pose as a legitimate vendor and through email exchanges let the appropriate accounting person know of new banking instructions. Believing the emails are legitimate, the accounting person makes note of the change. When the next legitimate invoice is received, the funds are routed to the fraudster's account.

Fraudsters will use an email address similar to the person being impersonated by changing or adding one letter. Unless you look closely at the address you will not readily detect the change. The recipients of such emails have no idea they are dealing with a fraudster. The FBI estimates that worldwide losses attributed to these schemes reached $5 billion.

What can a company do to avoid falling victim to these schemes? It can be thwarted by using an authentication/ verification protocol whenever requests for payments or changes to banking details are received. The most effective method is a call back to a known phone number to verify the authenticity of the request with the person or company that purportedly made the request. The phone call has to be to a predetermined number that you know is good, otherwise, if you call the number on the fraudsters email, you will end up speaking with the fraudster.

So make that call. Don't be afraid of the boss. Even if the boss is difficult to deal with - and no one wants to bother a difficult boss when he is out of the office – it is best to follow internal procedures.

Make that verification call.
Avoid a loss.

WHAT MAKES AN HRO AN HRO?

Classic Examples of HROs

AIR TRAFFIC CONTROL

Air traffic controllers play a "high stakes three-dimensional chess game" every day.

—USA TODAY

AIRCRAFT CARRIERS

"Flight operations at sea is the closest to the "edge of the envelope"—operating under the most extreme conditions in the least stable environment…"

—GOVLEADERS.ORG

NUCLEAR POWER PLANTS

"With nuclear power, the high energy density makes the potential hazard obvious…"

—WORLD NUCLEAR ASSOCIATION

5 TRAITS OF HIGH RELIABILITY ORGANIZATIONS

1 PREOCCUPATION WITH FAILURE HROs focus like a laser on failure; they give "continuous attention to anomalies that could be symptoms of larger problems."

- ☑ Never assume if a control succeeds in containing a failure, everything is right.
- ☑ Look deeper into incidents to find underlying causes.

"The absence of errors or accidents leads not to complacency but to a heightened sense of vigilance for the next possible failure." — Agency For Healthcare Research And Quality

2 RELUCTANCE TO SIMPLIFY HROs do not apply generalized terms to describe potential sources of failure.

Simple thinking: "The alarm failed so we should replace it with a new one."

HRO thinking: "What if the alarm's failure was caused by something deeper?"

"(HROs) appreciate the complexity inherent in the number of teams, processes, and relationships involved in conducting daily operations." — Agency For Healthcare Research And Quality

3 SENSITIVITY TO OPERATIONS HROs do not assume that the continuous outcomes will be the same as planned, assumed, or hoped for.

- ☑ Pay close attention to operations and maintain awareness of what is and isn't working.
- ☑ Don't make assumptions.
- ☑ Ask questions.
- ☑ Use data to make decisions and track outcomes.

"HROs recognize that the earliest indicators of threats to organizational performance typically appear in small changes in the organization's operations." — Joint Commission On Healthcare Accreditation

4 COMMITMENT TO RESILIENCY HROs are adaptable, learning organizations.

- ☑ Don't let failures disable your operations.
- ☑ Recognize emerging anomalies by keeping an open mind.
- ☑ React appropriately, even under unanticipated conditions.

"The hallmark of an HRO is not that it is error-free but that errors don't disable it." — Managing The Unexpected: Sustained Performance In A Complex World, Weick Ke, Sutcliffe Km

5 DEFERENCE TO EXPERTISE The "expert" is the person with hands-on knowledge of the operation at the point of failure.

- ☑ Give your experts access to upward reporting.
- ☑ Leaders must listen to those experts, regardless of seniority.

"...people in HROs know that in a crisis or emergency the person with greatest knowledge of the situation might not be the person with the highest status and seniority." — Agency For Healthcare Research And Quality

IS YOUR ORGANIZATION MOVING TOWARD HIGH RELIABILITY?

View Our Latest Slideshare Here: blog.lowersrisk.com/moving-toward-high-reliability/