GREAT AMERICAN & LOWERS RISK GROUP | ISSUE #42 | JULY 2018

FIDELITY/ CRIME OBSERVER

HUMAN CAPITAL RISKS

TABLE OF CONTENTS

5 STARTLING FACTS ABOUT HUMAN CAPITAL RISK

People are often referred to as the greatest asset of an organization. While this may be true for your organization, the greater truth is, people also represent an organization's greatest risks. The actions, inactions, and mere presence or influence of people, present a potential for loss across the spectrum of business activities.

Perhaps no source of risk is more perplexing, hurtful, and damaging than those caused by intentional harmful acts. Consider just a handful of startling facts:

1. ***30% of business failures are due to employee theft.***
2. ***Organizations lose 5% of revenue to 'fraud from within.'***
3. ***Workplace violence is the fastest-growing category of murder in the U.S.***
4. ***One in five American adults have experienced sexual harassment at work.***
5. ***80% of active shooter incidents occur in the workplace.***

Where there are people, there are risks. The actions taken by employees and even subcontractors representing your organization have a direct impact on the productivity, safety, and success of your organization. When those actions turn bad, either through negligence or intentional acts, the damage to people, brands, and profits can be significant. What are you doing to identify, prepare for, and mitigate your human capital risks?

Read Full Blog Here: blog.lowersrisk.com/human-capital-risk-facts/

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

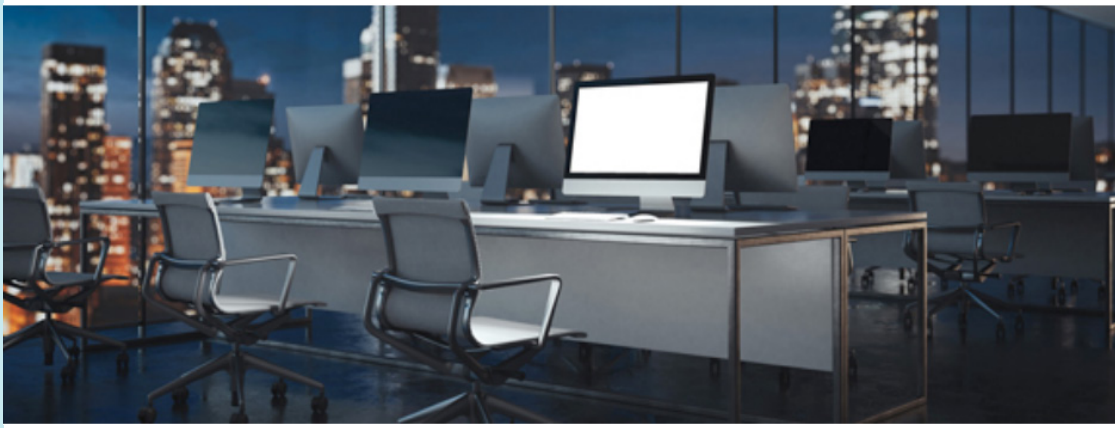
Dennis Burns, SVP
Fidelity / Crime Division
212.513.4017
dburns@GAIG.com
greatamericaninsurancegroup.com

LowersRiskGroup®
Protecting People, Brands, and Profits

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

THE RED FLAGS OF FRAUD

By: Tim Markey, Assistant Vice President, Crime Claims
Great American Insurance Group, Fidelity/ Crime Division



Research by the Association of Certified Fraud Examiners has demonstrated that there are behavioral indicators displayed by employees who perpetrate frauds. They found that in 85% of cases, fraudsters displayed at least one behavioral red flag and in 50% of cases they exhibited multiple red flags.

The six most common behavioral red flags include:

- **Living beyond means**
- **Financial difficulties**
- **Unusually close association with vendor/customer**
- **Control issues, unwillingness to share duties**
- **Divorce/family problems**
- **"Wheeler-dealer" attitude**

Indeed, several of these red flags were evident in this recent case.

Camilla Cardhappy, a former Chief Financial Officer and Treasurer for a family-owned construction company, was arraigned on federal charges for embezzling more than $1 million from her employer to pay for her personal expenses. Cardhappy was a childhood friend of the family that owned the company and was trusted implicitly. The investigation revealed that between 2010 and 2015, Cardhappy used her position as the **CHIEF FINANCIAL OFFICER AND TREASURER** of the construction company to **STEAL MORE THAN $1 MILLION** by abusing her corporate credit card and issuing dozens of checks to pay for her personal expenses, including nearly $250,000 in flights, cruises, and other vacation expenses, more than $100,000 in cash withdrawals, and more than $100,000 in retail purchases. She issued checks to pay for these expenses by forging the President's signature without authorization. The checks ranged from $4,500 to $17,000.

Cardhappy concealed her fraud by falsifying entries on the company's check register and general ledger. The payments were miscoded as legitimate expenses for various projects. In addition, the cover up was facilitated by the company's outside accountant –with whom she was having an affair. The accountant capitalized upon the company's trust of the CFO by falsifying audit reports he submitted annually. When the affair was revealed, Cardhappy's husband filed for divorce. Cardhappy faced further financial troubles after her accountant/lover lost his job and needed her to financially support him.

THE COMPANY'S TRUST IN THIS LONG TIME FAMILY FRIEND CLEARLY BLINDED THEM TO THE SEVERAL RED FLAGS demonstrated by Cardhappy's behavior. At the time they didn't realize it but looking back it struck them that Cardhappy lived beyond her means. She loved cruises and took them often, sometimes to exotic places. Then there were also the vacations to fancy resorts, private school and riding lessons for her daughter, nice clothing and jewelry, among other things.

Another red flag was her relationship with their accountant. Since they trusted her so much, they never realized that her close relationship with the outside accountant was a potential problem for them.

They were aware of her divorce but didn't think it was cause for alarm. They were more concerned for her mental wellbeing.

The owners of the company did wonder how she would get by as a single mother on one salary. They even offered temporary financial assistance if she needed it. How foolish did they feel when they discovered her embezzlement?

Of course, hindsight is always twenty-twenty. But knowing and perceiving the behavioral warning signs exhibited by fraud perpetrators can help organizations detect fraud and mitigate losses.

4 STEP APPROACH TO BUILDING YOUR BUSINESS CONTINUITY PLAN

To stay prepared, organizations must expect the unexpected. Business Continuity Planning (BCP) addresses the need to have contingency plans in place to deal with potential threats that can turn an organization on its head. Continuity planning is a necessary part of coming out on top in the face of the most challenging circumstances such as a natural disaster, a significant market crash, or a serious hit to a company's brand or reputation.

As a risk manager, CEO, or any party responsible for the long-term success of an organization, you need to have a plan in place to clearly outline what you would do if the worst were to happen tomorrow. Here are four phases to putting your BCP in place.

1. BUSINESS IMPACT ANALYSIS (BIA)

The first step to building your company's BCP is to consider the potential impact of each type of disaster or risk event that your company may face. For example, a company in the finance industry may consider the role of the stock market, data breaches, or the possibility of a fraud scandal. The BIA helps you discern which processes are the most critical to recover or initiate in a state of a disaster and assigns a monetary value to the protection of assets involved in specific business processes.

Key goals of the BIA should include:

1. ***Identifying the impact of uncontrolled events***
2. ***Prioritizing critical functions***
3. ***Establishing maximum tolerable outages***

2. RISK ASSESSMENT

Upon identifying the impact of the risks facing various functions across your business, the next step is to determine the potential magnitude of these risks. This is a critical assessment to perform, as it helps establish which risks should be most emphasized in the BCP. Priorities can be established by looking at which risks are most likely to occur to determine the breadth of coverage for your company's BCP. To do this, you can run a gap analysis to compare your company's current contingency plans against that of the proposed risks to identify any holes you need to fill. With knowledge of these gaps, you can analyze various threats to identify their respective impact.

To aid in this process, it is helpful to work from a list of potential emergencies or viable threats as well as the likelihood and impact of such events such as to personnel, assets, or monetary impact. These can help formulate different scenarios to plan for, such as natural disasters or terrorist threats, as well as minor events such a power outage.

A best-practice risk assessment report should cover the following:

- ***Summary of Business Operations***
- ***Risk & Vulnerability Analysis***
- ***Critical Support Infrastructure***
- ***Physical Environment***
- ***Recovery Time Objectives***
- ***Business Recovery Strategies & Priorities***

3. BUSINESS CONTINUITY PLAN PREPARATION

During this step, the BCP is developed, taking into account the likelihood, magnitude, and potential impact of the risks that were identified in the previous step. The BCP preparation stage will take it a step further by documenting strategies and procedures to maintain, recover, and resume critical business functions as quickly as possible. Part of this preparation will entail a list of procedures to address priorities for critical and non-critical functions, services, and processes.

The BCP should include:

- ***Business Operations***
- ***BCP Organization***
- ***Plan Activation & Operation***
- ***Preparation & Readiness Checklists***
- ***Emergency Operations***
- ***Facility Restoration & Relocation***
- ***Emergency Communications***
- ***Emergency Forms & Terms***
- ***Incident-Specific Response Checklists***

4. BUSINESS CONTINUITY PLAN TESTING AND TABLE TOP EXERCISES

Once a plan is established, it's time to put it to the test with table top exercises. During this final step, key staff members and management will come together to simulate their response to various emergency situations that were identified as likely risks. Using the procedures outline in the BCP, these exercises will identify gaps in the plans to improve them in a controlled setting. This process can also help establish the different roles and responsibilities across team members.

When it comes to risk mitigation, hope for the best but plan for the worst. Take your risk planning to the next level by getting started with your Business Continuity Plan.

Talk to a risk mitigation expert today.
www.lowersrisk.com

2018 SCTA CONFERENCE

OCTOBER 10-12, 2018

JOIN US TO PROTECT, STRENGTHEN, AND UNITE THE CASH-IN-TRANSIT AND CASH SERVICING INDUSTRIES.

The foremost conference in the cash servicing industry, the SCTA Conference attracts professionals and corporations in ATM servicing, cash handling/processing, transportation, and the safekeeping of cash and coin.

The theme of the 2018 SCTA Conference is "A State of Change," reflecting on the cash and transport industry's current evolution and the changes it could undergo in the next five years. The two-day event will feature informative sessions, networking opportunities, exhibits, and a keynote address by Jack Uldrich, an expert in helping organizations navigate unpredictability in the face of emerging trends.

LOCATION: WESTIN MICHIGAN AVENUE CHICAGO

At the Westin Michigan Avenue Chicago you're in the heart of Chicago, the Gold Coast neighborhood, and Lake Michigan. From the moment you step inside you feel the traditional ambiance of the welcoming lobby designed with granite and terrazzo.

909 N Michigan Ave, Chicago, IL 60611
Phone: (312) 943-7200

FEATURING A BOOKPLATE SPONSORSHIP

Get your company logo placed in Jack Uldrich's book, Higher Unlearning, which will be given to all conference attendees. This is an excellent way to spotlight your company.

For more information on sponsorship opportunities, preliminary agenda, booking a hotel, or to register please visit us at: http://scta.securetransportassociation.org/

[INFOGRAPHIC] THE STATE OF VIOLENCE IN THE CIT INDUSTRY

Robberies of armored CIT vehicles are a real risk faced by companies and their drivers. Violent robberies, which involve physical assault, guns, chemical sprays, and even murder, are quite another. Violent robberies are on the rise and have become a prevalent concern for armored carriers, even more so than in banks. The phenomenon is profound: while violent bank robberies occur in only 3.5% of all robberies, 49% of armored car robberies involve a violent act.

Armored car operators and personnel face a dual threat, as both the number of robberies and the presence of violence are on the rise. Strides have been taken to address these safety concerns, including the Hobbs Act, which establishes armored car robbery as a federal crime. However, findings indicate that this legal amendment has failed to deter the most violent criminals.

It is paramount for CIT operators to pro-actively address this rising threat. In our latest infographic, we present the most up-to-date research on armored car robberies and offer 8 ways to combat the threat of violent robberies.

View our latest infographic here: blog.lowersrisk.com/infographic-violence-cit-industry/