Ridgemark Insurance Services

MARCH 2021 | VOLUME 2 | ISSUE 3

NEWSALERT

Social Engineering Crime

Business Compromise Scams Growing Fast

BUSINESS COMPROMISE scams that use both technology and a human touch to steal funds from businesses are growing as criminals engage in social engineering tactics to dupe unsuspecting employees.

Businesses have lost millions of dollars to social engineering scams, where attackers impersonate a company president or executive who is authorized to approve wire transfers to trick employees into transferring funds into a fake client or vendor account.

According to the FBI's Internet Crime Complaint Center, in 2019 U.S. businesses were hit with an estimated 23,775 e-mail compromise scams that resulted in aggregate losses of $1.7 billion. Figures for 2020 are not yet available.

Vishing – or voice phishing – attacks have been growing. The FBI in January warned of an increase in vishing attacks targeting employees working remotely in the COVID-19 pandemic, and of the heightened risks companies face when network access and broadening of online privileges may not be fully monitored.

How to train employees

Providing practical employee phishing training is key to keeping your company safe. The following are activities and tips to help you train employees to stay vigilant.

ADVICE FROM THE FBI

- Consider instituting a formal process for validating the identity of employees who call each other.
- Restrict VPN connections to managed devices only (meaning not on employees' personal devices).
- Restrict VPN access hours.
- Employ domain monitoring to track the creation of or changes to corporate brand-name domains.

Remote workers should be vigilant in checking internet addresses, more suspicious of unsolicited phone calls and more assertive in verifying the caller's identity with the company, the FBI recommends.

When training staff, you should:

- Explain what vishing and phishing is, how it happens, and what risks it poses on a personal and company level.
- Explain the different types of phishing attacks.
- Train your workers in identifying signs of phishing attacks, like e-mails with poor spelling and grammar, incorrect e-mail addresses (for example BobS@Startbucks.com), and fraudulent URLs.
- Train your staff in recognizing phishing links, phishing attachments and spoofed e-mails. Additionally, your employees should know what steps to take after they identify a threat.
- Conduct simulations that send employees fake phishing e-mails. The results should be shared with them to show how they fell for the scam and the damage that being duped into clicking on a malicious link can cause.

See 'Commercial' on page 2

Ridgemark Insurance Services

Ridgemark Insurance Services

2130 Professional Drive, Ste 225,
Roseville, CA 95661

Phone: 916-306-1550
www.ridgemarkinsurance.com

If you would like to receive this newsletter electronically, e-mail us at:
info@ridgemarkinsurance.com

Expected COVID-19 Claims Surge Never Came

COVID-19 WORKERS' compensation claims have not been as widespread as insurers and ratings agencies around the country had predicted when the pandemic started exploding in early 2020.

Also, a large chunk of COVID-19 workers' compensation claims filed by workers nationwide have been rejected, with insurers often citing lack of proof that the illness was contracted in the workplace.

The insurance industry was bracing for a deluge of workers' comp claims when the seriousness of the pandemic became evident. This was especially true as more states passed laws requiring that essential workers be eligible for workers' compensation benefits if they contracted the coronavirus.

The laws introduced the presumption that if an essential worker came down with the disease, they had contracted it on the job.

Hundreds of thousands of COVID-19 claims were filed by workers around the country last year, but insurers were never overwhelmed. That's because the number of other, more typical workers' compensation claims tumbled dramatically as more employees were asked to work from home, while others were laid off in droves as plants shut down or business slowed.

With fewer people working on-site, the number of other workplace injuries and illnesses dwindled, experts say.

In the nine months ended Sept. 30, workers' compensation payments and liabilities fell 7.6% from the same period of 2019, according to the National Council on Compensation Insurance (NCCI), which is the rate-making agency in more than 30 states.

Rejected claims

As mentioned, a significant percentage of COVID-19 workers' compensation claims have been rejected. For example:

- In California, which has a law that extends the presumption that a case was contracted at work for anybody working on-site, 26% of the 93,470 COVID-19 claims filed in 2020 were denied.
- In Texas, which has no presumption for COVID-19, 45% of the 32,000 related workers' comp claims were denied, despite those workers testing positive.
- In Florida, which has given front-line workers who are state employees a presumption of eligibility, 22% of state employees' coronavirus-related workers' comp claims were denied last year, compared to 56% of cases for workers in the private sector. The NCCI also noted that fewer than 2% of COVID-19 workers' compensation claims cost more than $10,000.

Payouts lower than expected

Another factor is that even COVID-19 claims that were accepted, often did not end up costing the insurers as much as they expected to pay out because the majority of infected workers did not require any hospital stays or treatment.

Insurers also say that many claims were likely never reported in the first place, particularly when workers had mild or no symptoms. ❖

SURPRISING RESULTS

- 20% of COVID-19 medical claims had an inpatient stay.
- Of those claimants with an inpatient stay, 19% were in an ICU for some portion of their time in hospital.
- The average length of inpatient stays for COVD-19 medical claims was 7.5 days.
- The average cost per day was $5,400, totaling on average $38,500 per inpatient stay.
- COVID-19 medical claims requiring an ICU visit tended to incur longer and more expensive inpatient stays, at 11.5 days and $67,300 per inpatient stay, respectively.

Source: National Council on Compensation Insurance

Continued from page 1

Commercial Crime Insurance Can Help Recoup Losses

Insurance

As vishing and business e-mail compromise scams increase, more employers are seeking to add coverage in their commercial crime policies.

Typically, these policies have been used to cover losses for internal theft, but lately about 50% of claims are for losses related to phishing and vishing scams.

The price of social engineering coverage varies by risk and limit, but it can often be added to a crime policy as a rider.

One thing though: social engineering coverage will often have lower limits than a typical commercial crime policy. This is because of the risk of much larger financial losses than a company could expect from internal theft or white-collar crime perpetrated by an employee. ❖

Cal/OSHA COVID-19 Inspections Pick Up Steam

AFTER ISSUING emergency regulations in November, Cal/OSHA began to step up its enforcement of COVID-19 protections in California workplaces.

The types of business being cited cut across many sectors. Although most are focused on health care settings, the inspections are also sweeping up retailers, restaurants, fitness centers, agricultural operations, food processing and other manufacturing settings.

Since it issued the emergency regs to provide a framework for employers to reduce risks of their workers contracting COVID-19 while on the job, the workplace safety enforcement agency has issued citations to 75 employers, with proposed penalties totaling more than $1.54 million.

Most employers were cited for multiple COVID-19-related infractions.

Since Cal/OSHA started inspecting companies for failing to implement coronavirus safeguards last summer, it has issued $3.3 million worth of proposed penalties in total.

MOST COMMON CITATIONS

- Failing to effectively establish, implement and maintain procedures to correct unhealthy conditions related to COVID-19 that affected a business's employees.
- Failing to notify Cal/OSHA of a COVID-19 fatality.
- Failing to create a proper safety program.

WHAT'S PROMPTING INSPECTIONS

A complaint

Often it's either staff or a customer that contacts Cal/OSHA to complain about poor COVID-19 protections, as was the case when it received a complaint about a gym in Ventura.

Upon inspection, Cal/OSHA determined that the gym was not enforcing face covering use and physical distancing. It was cited for one willful-serious, two serious and six general violations.

Proposed penalties: $57,740.

A news report

Cal/OSHA cited a market in Oakland for multiple violations, including three serious. This followed an inspection after local media reported that 17 workers tested positive for COVID-19, one of whom was hospitalized.

Cal/OSHA determined that Cardenas Market had failed to adequately address the potential outbreak of the coronavirus among workers by implementing preventative measures. The business did not initially implement or require face coverings or masks, physical distancing or training of workers on coronavirus hazards. Cardenas Market also failed to immediately report a COVID-19-related serious illness.

Proposed penalties: $30,670.

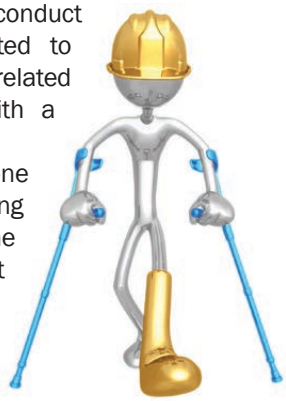
A fatality

A large agricultural concern was cited for multiple violations including two serious, following a fatality-initiated inspection after an employee was hospitalized and died from COVID-19 after working at a carrot field in Holtsville.

Cal/OSHA found that the employer had failed to implement safety protocols for its farm workers and failed to train them on the COVID-19 hazards and prevention.

Proposed penalties: $30,600.

An accident



Sometimes Cal/OSHA shows up to conduct an inspection of an accident unrelated to the coronavirus and finds COVID-19-related infractions as well. This happened with a retailer in Gilroy.

Cal/OSHA cited the shop for one regulatory and one serious citation following an accident inspection. It found that the employer had failed to immediately report a COVID-19-related serious illness, and to establish, implement and maintain an effective Injury Illness Prevention Program.

Proposed penalties: $15,125.

The takeaway

As you can see, Cal/OSHA will inspect any employer for possible infractions, particularly if there are complaints or news about an outbreak at a workplace. If you have not already done so and you have staff working at a physical location, you should immediately establish safeguards that are in line with Cal/OSHA's emergency regulations.

Remember too: Those regulations not only require you to protect workers against COVID-19, but to also report to Cal/OSHA and other authorities anytime there is an outbreak or a case in your workplace.❖

Supply Chain Disruption Lessons from Pandemic

BESIDES THE health and economic devastation that the COVID-19 pandemic has left in its wake, it has also caused supply chain disruptions that have affected a number of industries.

The fallout for companies of all types illustrates the fragility of most businesses' supply chains. The pandemic has left retailers with half-empty shelf space because product manufacturers couldn't keep operations going due to raw material or personnel shortages, while a number of carmakers and other manufacturers have had to suspend operations because of a global semiconductor shortage.

But it's not only large companies that suffer, and small businesses are especially vulnerable. That's why it's important that you have in place a solid plan for averting and dealing with disruptions to your supply chain if you rely on materials and inputs from outside vendors.

Here's what you can do to manage this growing risk.

Understand your supply chain

Start by identifying risks in your supply chain and develop ways to mitigate them.

FOUR MAIN EXTERNAL SUPPLY CHAIN RISKS

- **Flow interruptions** – Problems with the movement of goods and materials.
- **Environmental risks** – Economic, social, political, terrorism threat and weather-related factors that affect facilities and infrastructure. The pandemic falls into this category.
- **Business risks** – Problems caused by factors like a supplier's poor financial or general stability, or the purchase or sale of supplier companies by other entities.
- **Physical plant risks** – Problems at a supplier's facility. For example, a key supplier could have a machinery breakdown and/or regulators may shut the facility down.

Develop a plan

The best way to manage a supply chain disruption is to prepare for it. Start by undertaking a business impact analysis to prepare your company.

Form a team of key personnel to:

- Identify alternatives to key suppliers. One option is to contract with an alternative vendor in advance, so you can certify them and ensure they can ramp up if you lose a critical supplier.
- Model the impact of disruptions on your production and inventory for the four supply chain risks listed to the left. Think about how non-delivery of a key item would affect your operations.

Using that information, you can build contingencies for supply chain failures:

- Plan for how you would respond to all "what if" scenarios that could affect your operations. Be realistic about assessing your capacity to respond to these scenarios.
- Create a contingency plan for failure of any supply chain pillars. Identify the points at which you would need to execute risk-mitigating measures, like sourcing from other vendors or using new distribution channels.
- In advance, amass a contingency management team that will bridge the divide between your departments during disruptions. This team must include senior staff who are influential with top company decision-makers.
- Make sure your supply chain is flexible enough to deal with risks. Look at opportunities to address current supply chain bottlenecks; investigate alternative transportation network configurations or production systems.

The final backstop: insurance

You can address supply chain risks with business interruption insurance or contingent business interruption insurance.

Business interruption insurance. This coverage, which is often included in a commercial property policy, covers lost profits after a company's own facility is damaged by an insured peril.

Contingent business interruption insurance. This is often a policy rider that you can purchase. It covers lost profits if an insured peril shuts down a critical supplier, part of the transportation or distribution chain, or a major customer.

This coverage is triggered if there is:

1. Damage to property that prevents one of your suppliers from making products or delivering them.
2. Damage to property that prevents your customers from receiving your products. ❖