MINDFUL
INSURANCE SOLUTIONS INC.

RISK REPORT

APRIL 2021 | VOLUME 4 | ISSUE 2

Stimulus Plan Expands Business Assistance

THE $1.9 TRILLION American Rescue Plan Act (ARPA) that President Biden signed into law on March 11 contains a number of provisions intended to help small businesses and other organizations hurt by the pandemic.

Foremost, it includes additional Paycheck Protection Program (PPP) loans to struggling businesses, and a number of special grants to companies in industries that have been especially hard hit, including restaurants, movie theaters, concert spaces and museums.

The measure also includes provisions extending a number of tax credits to employers affected by the pandemic, in order to make it easier for people laid off during the health emergency to access COBRA coverage after they lose their jobs and their health coverage.

ARPA opens up a new opportunity for businesses that have been hurt by the pandemic to access financial aid to keep their doors open and stay viable. Many of the programs build on ones introduced earlier in the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) and extended by the Consolidated Appropriations Act of 2021 (CAA).

PPP extended

The law authorizes another $7.25 billion for the Paycheck Protection Program, which offers forgivable loans to small firms and other organizations that have been hit by the pandemic.

These loans are forgivable if 60% of the funds are used on payroll and the rest pays for mortgage interest, rent, utilities, personal protective equipment or certain other business expenses.

While the legislation set the deadline to apply for March 31, the deadline was extended until June 30 after Congress passed supplemental legislation.

Other assistance

There are a number of other provisions of the new law aimed at providing financial aid:

- $10 billion for state governments to help leverage private capital and make low-interest loans and other investments to help their small businesses recover.
- $15 billion to the Economic Injury Disaster Loan grants program to be given to small businesses in underserved areas, especially minority-owned enterprises.
- $29 billion for financial relief grants to restaurants. The maximum grant size will be $5 million for restaurants and $10 million for restaurant groups. The Small Business Administration will administer these grants.
- $15 billion will be added to the Shuttered Venue Operators Grants program, which was launched by the CARES Act. More funds will be made available to museums, theaters, concert and other venues that had to shut down due to COVID-19-induced restrictions.This program has not yet launched.

See 'Credit' on page 2

CONTACT US

MINDFUL
INSURANCE SOLUTIONS INC.

2043 ANDERSON RD, SUITE C
DAVIS, CA 95616

Toll Free: 877-223-4437
Fax: (530) 419-4811

E-mail: info@mindfulins.com

License #0167525

Cyber Insurance

As Attacks and Costs Mount, Rates Climb Higher

CYBER INSURANCE rates are going to increase dramatically in 2021, driven by more frequent and more severe insured losses, according to a recent industry study.

The report by global insurance firm Aon plc predicted that rates would jump by 20% to 50% this year due to two main factors:

1. Cyber attacks are becoming more frequent

While publicly disclosed data breach/privacy incidents are actually occurring less often, ransomware attacks are exploding in frequency.

Ransomware incident rates rose 486% from the first quarter of 2018 to the fourth quarter of 2020. The comparable rate for data breach incidents fell 57% during the same period. The incident rates for the two types of events combined rose 300% over the trailing two years.

2. The costs of these attacks are growing

The average dollar loss increased in every quarter of 2020. Ransomware attacks were particularly severe – many of them resulted in eight-figure losses. Others may grow to that level as business interruption losses are adjusted and lawsuits against insured organizations proceed.

The combination of more frequent and more costly losses is a recipe for higher rates.

Cyber insurance rates continued increasing in 2020, with rises of between 6% and 16% in the last four months of the year.

In January 2021, most of the top 12 cyber insurance companies told Aon they were planning more drastic rate hikes. Nearly 60% reported that they would be seeking rate increases of 30% or more during the second quarter. None of them expected increases less than 10%.

New underwriting criteria

When insurers evaluate cyber insurance applicants, they will be particularly concerned with the organization's overall cyber risk profile, its cyber governance and access control practices, and its network and data security. Prior loss history will be less important because the frequency of attacks is growing so quickly.

Some insurers may also cap how much they will pay for ransomware losses, or even exclude them entirely. They may also increase the waiting periods before coverage begins to apply.

WHAT BUSINESSES CAN DO

To improve your chances of getting more favorable pricing and coverage, the report recommends that you focus on:

- Reducing the risk of cyber losses.
- Measures to keep data private.
- Building an internal culture of cyber security.
- Preparing for ransomware attacks and disaster recovery planning.
- How your contracts and insurance will respond to a supply chain security breach.
- Understanding primary and excess coverage terms and communicating primary terms to excess insurers.

Continued from page 1

Employee Retention Credit Extended Until Year's End

Tax credits

Originally enacted under the CARES Act and CAA, the Employee Retention Credit (ERC) lets certain employers take advantage of a tax credit for qualified wages paid to employees.

The CARES Act capped the ERC at $5,000 per employee for 2020. The CAA, passed in late 2020, expanded the ERC to apply to qualified wages made between Jan. 1 and June 30 this year. It also increased the maximum amount of the credit to $7,000 per employee per quarter.

The new stimulus law extends the ERC through the end of this year. That means that eligible small firms can take a tax credit of up to $28,000 per employee for 2021.

Who is eligible: Businesses that were either fully or partially suspended as a result of COVID-19-related government orders that restricted their ability to operate and generate sales. Also, any business that has gross receipts that are less than 80% of gross receipts for the same calendar quarter in 2019.

ARPA also makes eligible for the tax credit any start-up businesses that also suffered revenue losses as a result of the pandemic.

In addition, ARPA extends through September the availability of paid leave credits to small and midsize businesses that offer paid leave to employees who may take leave due to illness, quarantine or caregiving due to the pandemic and any closure orders.

Employers that offer paid leave to workers who are sick or in quarantine can take dollar-for-dollar tax credits equal to wages of up to $5,000.

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.

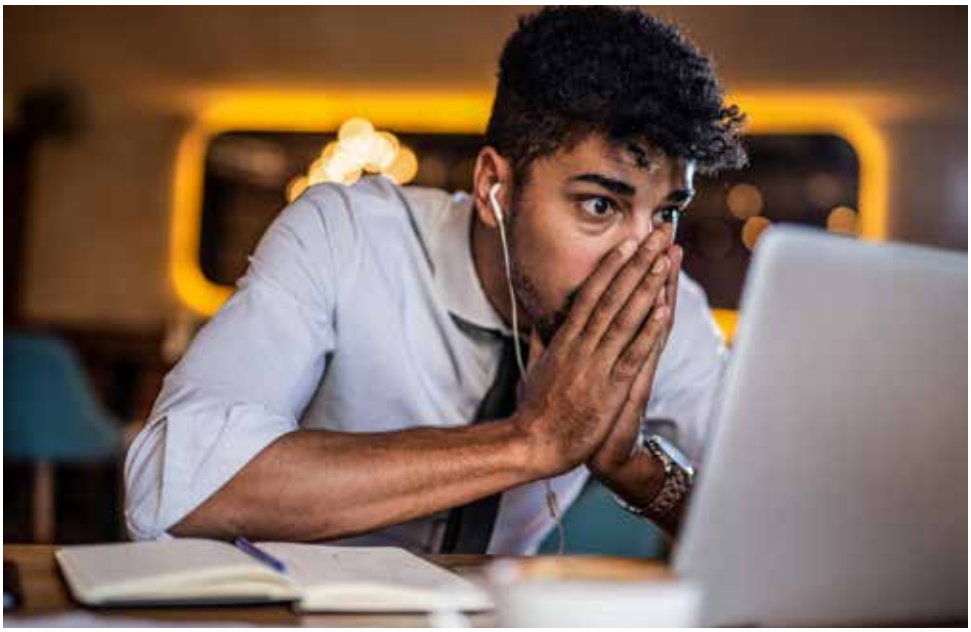
Vishing – or voice phishing – attacks have been growing. The FBI in January warned of an increase in vishing attacks targeting employees working remotely in the COVID-19 pandemic, and of the heightened risks companies face when network access and broadening of online privileges may not be fully monitored.

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.

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.

Produced by Risk Media Solutions on behalf of Mindful Insurance Solutions, Inc. This newsletter is not intended to provide legal advice, but rather perspective on recent regulatory issues, trends and standards affecting insurance, workplace safety, risk management and employee benefits. Please consult your broker or legal counsel for further information on the topics covered herein. Copyright 2021 all rights reserved.

Risk Management

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.