Ridgemark Insurance Services

APRIL 2022 | VOLUME 3 | ISSUE 4

NEWSALERT

Growing Threat

Funds Transfer Fraud Hits Small Firms the Hardest

WHILE RANSOMWARE is making the headlines as the major cyber threat, small and mid-sized businesses are increasingly being targeted by lower fraud that dupes them into wiring criminals funds, according to a new report.

These funds transfer fraud crimes involve hackers gaining access to a firm's mailbox and extracting payments that go into their accounts.

Companies should have in place proper systems safeguards to combat these attacks, and that includes regularly training staff on how to identify these attempts to steal funds.

By The Numbers

69%	Average jump in losses from funds transfer fraud from 2020 to 2021
105%	Average jump in small firms' losses from funds transfer fraud from 2020 to 2021
$309,000	Average initial losses from funds transfer fraud for small firms in 2021

Source: Coalition's "2022 Cyber Claims Report"

How it works

Criminals will often try to penetrate your servers by sending "spearphishing" e-mails. These messages look like they're from a trusted sender to trick victims into revealing confidential information.

They may also send malicious e-mails in the hope that an employee clicks on a bogus link. The link then releases malicious software that infiltrates company networks and gains access to legitimate e-mail threads about billing and invoices.

Once the criminals have access to your business mailbox, they can manipulate your contacts and modify payment instructions. They may also use their access to your systems to send e-mails that appear to come from a known source making a legitimate request.

Protecting your enterprise

- Don't click on anything in an unsolicited e-mail or text message asking you to update or verify account information. Look up the company's phone number on your own (don't use the one a potential scammer is providing), and call them to ask if the request is legitimate.
- Carefully examine the e-mail address, URL and spelling used in any correspondence. Scammers use slight differences to trick your employees and gain your trust.
- Be careful what you download. Instruct your staff to never open an e-mail attachment from someone they don't know, and to be wary of e-mail attachments forwarded to them.
- Set up two-factor (or multi-factor) authentication on your accounts.
- Verify payment and purchase requests in person if possible, or by calling the person to make sure it is legitimate. You should verify any change in account number or payment procedures with the person making the request.
- Be especially wary if the requestor is pressing you to act quickly.

Source: Federal Bureau of Investigation

See 'Coverage' 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

Retirement Savings Law

CalSavers Registration for Small Employers

THE DEADLINE is fast approaching for employers with five or more workers in California, and who do not already offer their employees a retirement plan, to register their staff for the CalSavers Retirement Savings Program.

Only California employers that do not offer retirement plans are required to register for CalSavers and there are different registration deadlines depending on employer size, staggered over a few years as follows:

Employers with 100 or more workers – The deadline for registration was June 30, 2020.

Employers with 50 or more workers – The deadline for registration was June 30, 2021.

Employers with five or more workers – The deadline for registration is June 30, 2022.

Employers can register anytime to start the program for their workers. Firms with fewer than five employees are exempt, but they too can sign their workers up for CalSavers.

Employers that don't provide a retirement plan for their workers, and who fail to register, can face a penalty of $250 per employee, as well as additional penalties for sustained noncompliance.

If you already have a qualified retirement plan for your employees, you do not have to participate.

Qualified retirement plans

- Qualified pension plans
- 401(k) plans
- 403(a) plans
- 403(b) plans
- Simplified Employee Pension (SEP) plans
- Savings Incentive Match Plan for Employees (SIMPLE) plans
- Payroll deduction IRAs with automatic enrollment.

How CalSavers works

Participating employers will deduct a default rate of 5% of pay from the paycheck of each employee at least 18 years old and deposit it into the individual's CalSavers account. Employees can choose other rates as well.

Employee participation is voluntary, and they can opt out at any time. Regardless of whether any employees want to sign up for a plan, applicable employers are required to register and offer the program to all current employees and new hires.

The deduction amount will automatically escalate one percentage point each year to a maximum of 8%, unless the individual employee elects a different amount, elects out of auto-escalation or completely opts out of the program.

Business owners who are employees of their business can also participate. Business owners who are not employees may enroll as an individual and make automatic contributions every month. There are no costs for businesses to sign up and facilitate the program for their employees.

Employers can register here. Once set up and employees have signed up, the employer will be responsible for taking off the chosen deduction for each employee and transferring it to CalSavers at each pay period.

For employees

A CalSavers account is a personal Roth Individual Retirement Account (Roth IRA) overseen by the CalSavers Retirement Savings Investment Board. Here's some information employees need to know:

- A portion of their pay is automatically deducted after taxes are taken out and transferred to an IRA that belongs to them.
- Employees can customize their account by setting their own contribution rate (between 1% and 8%), as well as choose the investments they want to put their money in.
- The account is portable: They keep it if they leave their job. ❖

Continued from page 1

The Best Coverage Option Is a Commercial Crime Policy

Insurance options

The best option for coverage is a commercial crime insurance policy.

Most of these policies cover acts like:

- Employee dishonesty
- Computer and funds transfer fraud
- Forgery or alteration
- Money and securities theft
- Theft of client's property.

Some policies may exclude funds transfer fraud, or they may have lower sublimits for such acts. In such cases you may need to get a policy extension to cover the risk.

There is also cyber liability insurance, which covers direct losses resulting from cyber crime. But these policies will often exclude coverage for social engineering attacks, which are the kinds that the criminals behind funds transfer fraud use.

You may be able to purchase a rider to your cyber liability policy that would cover these crimes. ❖

Planning Ahead for Equipment Failures Can Save You

AS A BUSINESS owner you already know you need to protect against and plan for external supply chain risks. These risks are often out of your control as they can affect suppliers or transportation providers, as well as transportation networks and infrastructure.

However, you also have internal supply chain risks, which you are better able to control. These risks can affect a variety of businesses from manufacturers to retailers and restaurants – and any business that has some type of revolving stock.

It could be vital to the survival of your business that you prepare for internal risks such as machinery and equipment breakdowns.

Knowing the right steps to take ahead of time can save you from making a bad situation worse or significantly delaying the resumption of operations. All of that, of course, amounts to extra costs for your operation, including the potential for lost revenues.

If you prepare for a failure of a key piece of equipment or machinery, you also won't be scrambling trying to figure out your next step in times of internal disruption or crisis. Making decisions at such times can often lead to more problems and costs.

Your risk management plan to deal with such failures should include:

1. A list of key equipment

- Production machinery, including gear sets, motors, compressors, belts and fans.
- Boilers and pressure vessels.
- IT and communications systems, including wiring and cables.
- Electrical equipment or system, including transformers, switch boxes, cables, wiring and motors.

2. An inventory of spare parts

Optimally, you should keep all the key spare and replacement parts for your main systems on site. You can ask the manufacturers or service companies of those systems to assist you in having an emergency inventory on hand.

Still, it may not be feasible to have all items on site. In that case, you should compile a list of the other parts that could break and need replacement, and how to quickly order them from the correct supplier. You should include on this list the cost of those items and delivery times – and update the list at least every year.

3. Plan for renting replacement equipment

As part of your planning, you should obtain quotes from companies that rent out the same type of equipment or machinery that you use, and update the quotes every year. The quotes should include all pricing like transportation and set-up fees, as well as estimated time from ordering to delivery and start-up.

Don't forget to include alternative suppliers.

4. Repair firms

You should also have at the ready information on the various contractors that are able to repair equipment that's broken down. The information should be listed by equipment item and should include contractor capabilities, contact information and availability.

Again, you should update this information every year.

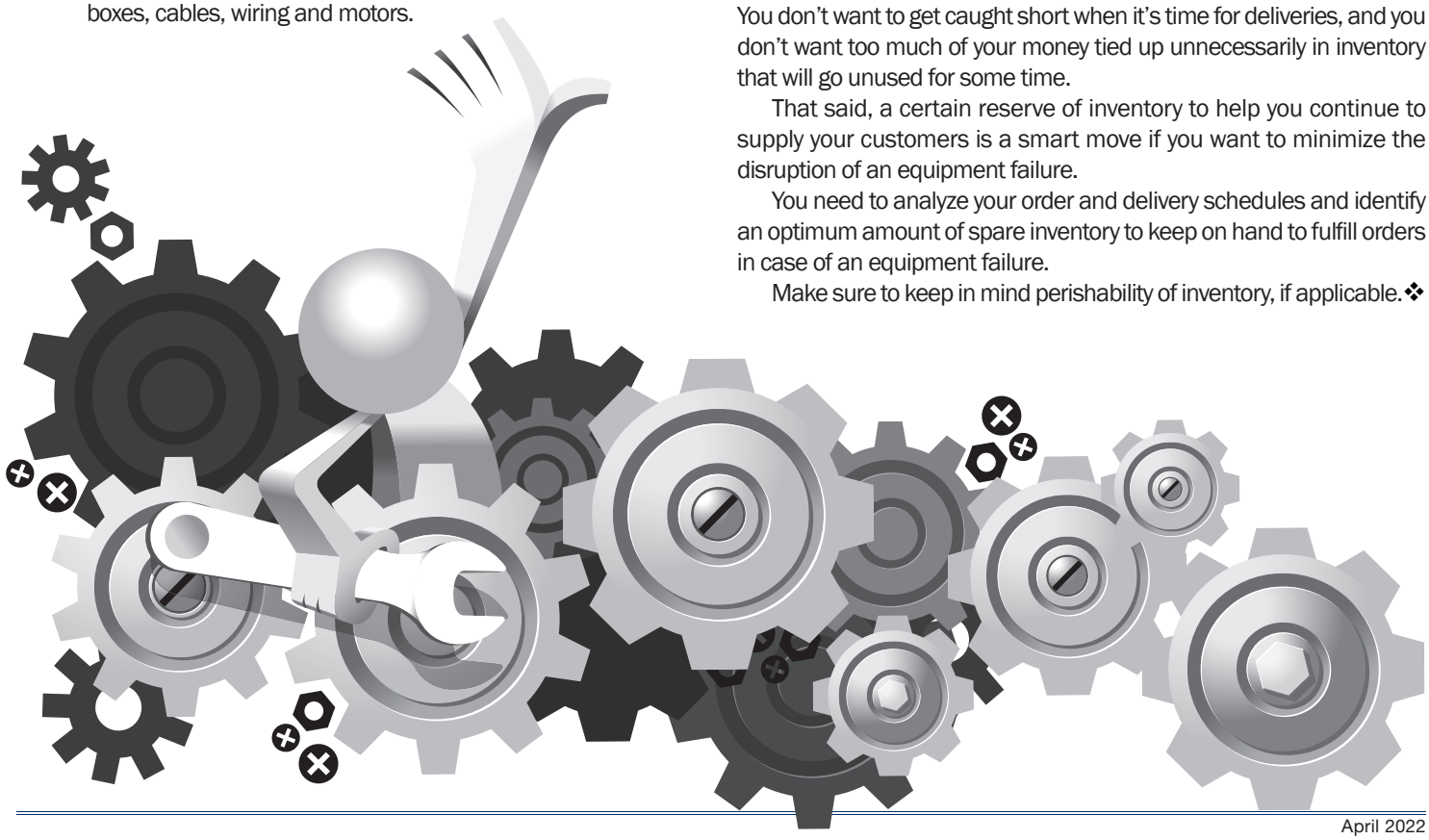
5. Inventory

The dilemma for many businesses is how much inventory to carry. You don't want to get caught short when it's time for deliveries, and you don't want too much of your money tied up unnecessarily in inventory that will go unused for some time.

That said, a certain reserve of inventory to help you continue to supply your customers is a smart move if you want to minimize the disruption of an equipment failure.

You need to analyze your order and delivery schedules and identify an optimum amount of spare inventory to keep on hand to fulfill orders in case of an equipment failure.

Make sure to keep in mind perishability of inventory, if applicable.❖



Wage & Hour Claims Loom as Remote Work Grows

WITH MANY companies having decided to allow staff to work remotely permanently or split time between working at home and in the office, employers have to be especially careful about timekeeping and complying with wage and hour laws.

That includes requiring staff to show they take meal and rest breaks and that they are compensated for overtime when they are asked to work extra hours.

The lines between work and home life can often blur for remote workers and it's not unusual for people to work at unusual times when telecommuting. But it's important that you set rules for your employees to ensure they are not working more than they should, particularly for nonexempt employees.

Also, because time can pass quickly when working remotely, it's easy for employees to work past quitting time because they lack the visual clues of others leaving the office at 5 pm.

If you fail to keep tabs on hours worked, meal breaks and rest breaks, your organization could be sued by employees who feel cheated – or face enforcement action by the state.

What you can do

To avoid that, here are some tips you may want to consider:

Keep a general schedule for workers – By creating a schedule for employees to follow, it will be easier for managers and supervisors to monitor their hours. Require staff to follow the schedule and take meal and rest breaks as if they were in the office.

Require them to record their time – There are a number of time-tracking applications and tools available to employers who have remote workers.

An off-the-shelf app can be easily installed on your employees' computers for them to log into when they start and finish work and take breaks.

These apps also help you keep track of any overtime they may work.

Closely monitor employees for overtime worked – One of the biggest risks in the wage and hour arena is not paying workers for overtime. This mistake is much easier to make when you have staff who work remotely.

Don't run afoul of overtime laws. Carefully monitor any and all overtime your staff logs.

Check in with your workers – A friendly reminder never hurts. You may want to connect with your employees on occasion to make sure they are taking scheduled paid rest breaks as well as their lunch breaks in accordance with state laws.

All your staff should have a copy of your meal and rest break policy, which should be written in clear language to reinforce the importance of taking scheduled breaks.

The takeaway

If you have staff who work from home full-time or a few days a week, inform them that they need to track their time, take required breaks and report any overtime they work.

This is most important for nonexempt staff, whom you are required to pay overtime if they work more than eight hours a day. ❖