Shaw Insurance Services REPORT
SEPTEMBER 2024
VOLUME 16 | ISSUE 9

Software Outages & Cyberattacks

Firms Often Have No Recourse After Costly Events

LATELY THERE'S been a series of high-profile cyberattacks and outages on software that organizations use to run their operations, causing major disruptions to businesses, sometimes hamstringing their ability to function.

The most recent example is the CrowdStrike cyber-security software outage that affected some 8.5 million businesses, most notably airlines, which had to cancel thousands of flights globally after their systems went down and they were unable to restart them.

There are a number of software solutions and programs that businesses use in their day-to-day operations and depending on how much they rely on one, a disruption could have costly implications, including the inability to function. There are lessons to be learned from a few massive events in the last year alone.

Three big and costly events

CrowdStrike outage – CrowdStrike, a cyber-security vendor, in July sent out a faulty update to its security software that caused widespread problems with Microsoft Windows computers running the software. The massive outage, which disrupted airlines, financial services and many other industries, caused an estimated $5 billion in financial losses.

Within hours, CrowdStrike discovered the error and sent out a fix, but because many affected computers had to be fixed manually, outages continued for weeks for some businesses.

CDK Global cyberattack – CDK Global in June was hit with back-to-back cyberattacks, forcing it to shut down its auto dealership management platform which some 15,000 showrooms around the country use to conduct most of their day-to-day operations.

Dealerships were forced to go back to old-fashioned pen and paper and other workarounds as they were unable to access CDK's services like e-signing, appointment scheduling — and customer records in some cases.

Change Healthcare ransomware attack – In February Change Healthcare, the payment clearinghouse software vendor that handles $1.5 trillion worth of transactions between health insurers, pharmacies, hospitals and patients, shut down its system after a huge ransomware attack that stole patient data and encrypted company files.

The downtime cost an estimated $2 billion as patients were unable to pay for their prescriptions at the pharmacy and payments from insurers to providers and pharmacies were also disrupted.

What businesses can do

All three of the above software vendors have been sued as a result of these events. But legal experts say that it will be difficult for affected businesses to sue CrowdStrike in particular, and win, as the grounds for litigation would be murky. Was it breach of contract? Fraud? Negligence?

And contract terms are not conducive to a large settlement in most software and platform outages. While contracts vary from customer to customer, the general terms and conditions will often limit their liability only to the amount that a customer pays for its service.

See 'Keep' on page 2

Workers' compensation

How to Streamline Your Insurance Policy Audit

ARE YOU due for a workers' compensation premium audit? Audits are how insurance rates are determined, and it's possible that an audit will uncover information that can actually save you money — or not if you've hired additional staff and haven't notified your insurer.

In any case, it pays to be prepared and you can do so with the following tips:

Note staffing changes – Let us know when there are changes in your staffing, payroll or areas of operation. This is important not just at audit time, but all the time. Your rates are based on variable rating information, including the number of employees, job classifications and the states in which you operate. Updated information results in more accurate premium assessments.

Get your records ready – Your auditor will need to see records such as federal and state tax returns, ledgers, checkbooks, contracts and employee or contractor tax documents. If you prepare your records in advance, you'll speed up the audit process.

Gather all payroll information – Make sure you break out various types of compensation in your records.

For example, to set your premium, we consider pay but not contributions to employee benefits packages and other perks, so it's important to make sure your records are clear on the various types of compensation.

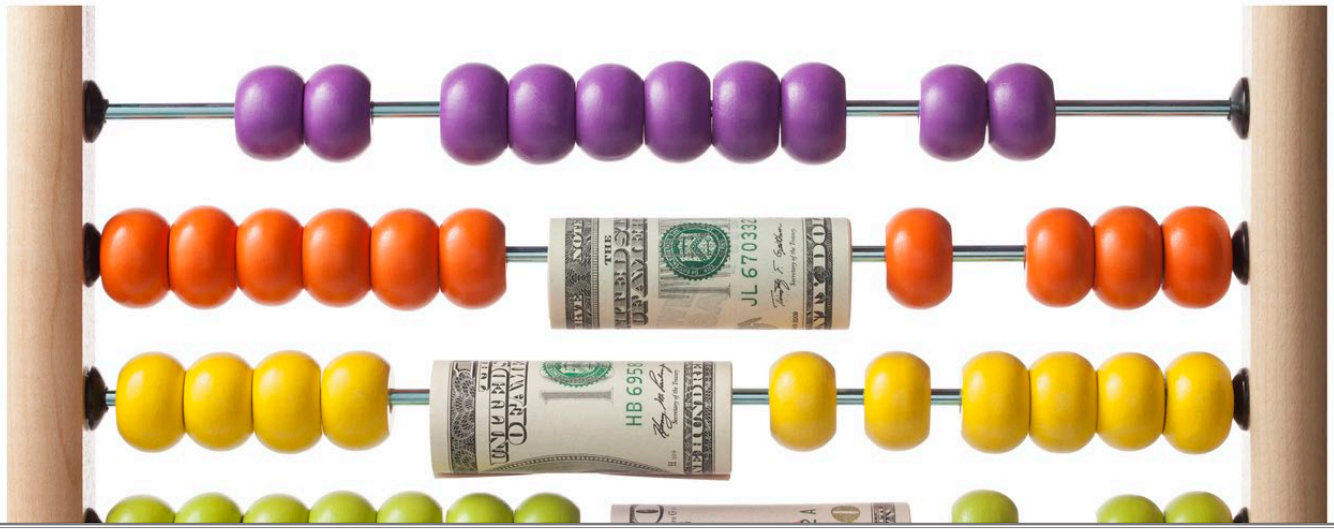
Also make sure overtime pay is clearly defined since it's classified as regular pay for workers' compensation insurance purposes.

Ensure that contractors have their own insurance – This is important not only from an audit standpoint, but from a liability perspective as well. If an uninsured contractor has an accident while performing work on your behalf, you can be held liable. If an audit identifies contractors for whom you don't have certificates of coverage, you can be charged for their premiums.

Remain on hand to answer questions – As your auditor reviews your material, he or she may have questions or need additional data. If you are available to provide answers, your audit will be completed more quickly.

The takeaway

By following these tips, you'll be more prepared for your workers' compensation premium audit. A fast, efficient audit process can save time for both you and your auditor, so it pays to be prepared. ❖



Continued from page 1

Keep Customers Informed About the Situation

After a outage like the one that affected CrowdStrike in July, businesses can take a number of steps to reduce the risk of future disruptions and maintain customer trust.

Phased updates: Deploy updates to a small percentage of devices first to reduce the risk of disruption if the update is flawed.

Simulation exercises: Run exercises to identify the most likely and disastrous IT crises, and develop a response.

Open communication: Keep customers informed about the situation and expected resolutions.

Customer service: Prepare customer service teams to handle inquiries and concerns from clients and vendors.

Compensation: Offer compensation or incentives to affected customers.

Consider alternatives: Explore other cyber security solutions from established companies that have a long track record of reliability and resilience against attacks. ❖

Internal Threat

Businesses Suffer as Employee Theft Grows

ORGANIZATIONS AROUND the world lose an estimated 5% of their annual revenues to occupational fraud, according to a survey by the Association of Certified Fraud Examiners (ACFE).

The association estimates that U.S. businesses lose some $50 billion a year to employee theft, and that 75% of employees have stolen at least once from their employer — and 37% have stolen at least twice. So, what can your organization do to avoid falling victim? The U.S. Small Business Administration and the ACFE recommend that companies:

Use pre-employment background checks – Basic pre-employment background checks are a good business practice, especially for employees who will be handling cash, high-value merchandise, or have access to sensitive customer or financial data.

Be aware that laws on background checks vary from state to state and if you go too far in your check, you may be in breach of the law and risk being sued. Recently the U.S. Equal Employment Opportunity Commission raised concerns that criminal background checks may disproportionately discriminate against some racial groups.

Check candidate references – Make a practice of calling all references, particularly if they are former employers or supervisors.

If your candidate has a history of fraudulent behavior, then you'll want to know about it before you hand them a job offer.

While some former employers may be loath to tell you anything bad, they will often give you clues in the conversation that the employee may have had some problems.

Implement a fraud hotline – Occupational fraud is far more likely to be detected by a tip than by any other method.

More than 40% of all cases were detected by a tip — with the majority of them coming from employees of the victim organization. There are several providers of hotline services that can help implement an anonymous tip-reporting system for businesses of all sizes and industries.

Conduct regular audits – Regular audits can help you detect theft and fraud and can be a significant deterrent to fraud or criminal activity, because many perpetrators of workplace fraud seize opportunity where weak internal controls exist.

Recognize the signs – Studies show that perpetrators of workplace crime or fraud do so because they are either under pressure, feel underappreciated or perceive that management behavior is unethical or unfair.

Warning Signs

Some of the potential red flags to look out for include:

- Not taking vacations. Many violations are discovered while the perpetrator is on vacation.
- Being overly protective or exclusive about their workspace.
- Employees that prefer to be unsupervised by working after hours or taking work home.
- Financial records sometimes disappearing.
- Unexplained debt.
- An employee living beyond their means.

Set the right management tone — One of the best techniques for preventing and combating employee theft or fraud is to create and communicate a business climate that shows that you take it seriously. You may want to consider:

- Reconciling statements on a regular basis to check for fraudulent activity.
- Holding regular one-on-one review meetings with employees.
- Offering to assist workers who are experiencing stress or difficult times.
- Having an open-door policy that gives employees the opportunity to speak freely and share their concerns about potential violations.
- Creating strong internal controls.
- Requiring employees to take vacations.

You should also treat unusual transactions with suspicion and trust your instincts. ❖

Employee Dishonesty Insurance

Employee dishonesty insurance coverage – sometimes referred to as fidelity bond, crime coverage or crime fidelity insurance – protects a small business employer from a financial loss as a result of fraudulent acts by employees.

The financial loss can be caused by an employee's theft of property, money or securities owned by the small business.

Lawsuit Risk

More Businesses Sued Over Disabled Website Access

BUSINESSES WITH a web presence, particularly those that are consumer-facing, are increasingly being sued over website accessibility issues that prevent visually impaired individuals from using a website.

While the number of such cases has been growing, 2,281 website accessibility lawsuits were filed nationwide in 2023, down from 2,387 the prior year and 2,352 in 2021, according to a report by *Accessibility.com*, a firm that helps businesses make their websites usable for certain disabled individuals.

The drop in cases actually filed is due to more organizations settling with law firms without going to court, in light of the fact that there was an 18% year-on-year increase in demand notices in 2023, the report concludes.

What is website accessibility?

Website accessibility refers to the extent to which a site can be used by individuals with disabilities. This can include people who are blind or have low vision, those who are deaf or hard of hearing, and people with mobility impairments, cognitive disabilities or other disabilities.

The Americans with Disabilities Act allows individuals with disabilities to bring lawsuits against businesses directly. A plaintiff can seek injunctive relief, such as asking for a court order requiring the website to be changed as well as attorneys' fees or costs. However, the ADA does not permit the recovery of monetary damages in these cases.

That said, many states, including California and New York, have enacted laws allowing individuals to recover monetary damages for disability discrimination. Courts in both states have ruled that websites are places of public accommodation akin to establishments with physical locations, and, thus, are subject to the ADA.

As a result, more than 85% of website accessibility lawsuits are filed in those two states, according to the *Accessibility.com* report.

There are indications that filing these types of lawsuits has become a moneymaker for a few law firms and individuals.

Follow the Money to CA, NY

- New York had nearly 73% of all the cases filed nationwide, followed by California and Illinois.
- Over 69% of all website accessibility lawsuits were filed by five law firms out of New York and California.
- Almost 16% of website accessibility lawsuits in 2023 were filed by five plaintiffs. One of them filed more than 105 lawsuits that year after filing 108 in 2022. The report found that four other individuals filed between 52 and 78 cases apiece in 2023.

What should businesses do?

Most of these lawsuits cite the "Web Content Accessibility Guidelines," published by the World Wide Web Consortium. While these guidelines are advisory only, they have become the standard to follow when making websites accessible to individuals with disabilities.

There are widgets that can be installed on websites to ensure they comply with the WCAG, but even so, 933 lawsuits filed in 2023 were against businesses that had installed such widgets on their websites.

Experts recommend:

- Regularly checking your website and digital content to ensure it is accessible to individuals with disabilities.
- Ensuring that your website complies with the latest WCAG guidelines and includes a general statement regarding accessibility and a clear indication of how to contact your company if an issue with accessibility arises.
- If necessary, hiring an outside vendor that can bring your website into compliance with the WCAG guidelines.
- If you receive an ADA demand letter or complaint, you should consult with attorneys who are experienced in these types of cases. ❖