HEFFERNAN INSURANCE BROKERS
Because You're Different

News You Can Use

Feb. 2016 Volume 4, Issue 4

BUSINESS INTERRUPTION

How to Cope with System Failures, Cyber Attacks

AS BUSINESSES become ever more connected and rely on their networks, websites and outside cloud services to conduct their operations, failure on any of these fronts poses a serious risk.

Your network, websites and cloud services can go down for various reasons like system crashes, hardware or electrical failures, or cyber attacks. Any of these can disrupt or completely freeze your operations, depending on how much your organization has gone digital.

With these risks growing, you need to have plans for keeping your operations humming along should you encounter an incident.

This is important because every minute your site or network is down is another minute you could be making money.

Finally, you should consider cyber insurance, which can cover the business interruption costs from system failures, cyber attacks and cloud service failures.

How cyber attacks happen

Cyber criminals often try to gain access to a company's network through weaknesses in the system. They do this through hacking or sending bogus e-mails urging recipients to click on a link (and surprisingly many do).

There are many ways criminals launch attacks that can freeze your operations:

- Malicious code that renders your website unusable.
- Distributed denial of service attacks that make your website inaccessible to both employees and customers.
- Viruses, worms or other code that deletes critical information on a business's hard drives and other hardware.

If any of these occur, your operations could be disrupted or completely shut down, leaving you scrambling. And if you run a small organization without a dedicated IT staff, the effects can multiply for you.

Defenses you can implement

You can reduce your chances of business interruption due to a cyber attack and network failure by following these tips:

- Create a formal, documented risk management plan that encompasses all of your systems, including each of their weaknesses, the data they store and processes. This plan should also rank each system's importance to your organization, so you know where to focus your resources.
- Make sure all firewalls and routers are secure and kept up to date to help defend against a cyber attack.
- Implement a cyber security policy that educates employees about the damage a cyber attack can cause and teaches them how to identify malicious e-mails and links. Your policy should also include rules for personal mobile devices and for accessing personal e-mail and social media accounts from work computers.
- Install software updates for your operating systems and applications when they become available.

See 'Disruption' on page 2

HEFFERNAN INSURANCE BROKERS

If you have any questions regarding your coverage or our products, please call us at one of our offices:

Walnut Creek
San Francisco
Menlo Park
Portland
St. Louis
Petaluma
Los Angeles
Orange County
New York

Sales: 877-731-7905
Service: 800-234-6787

MEDICAL MARIJUANA

Court: Okay to Fire Pot User Who Fails Drug Test

AS MORE states legalize marijuana for personal or medical use, employers have grown increasingly concerned about what they can and cannot do to enforce their existing drug policies.

A federal court in New Mexico has dismissed a case brought by an employee who was terminated after testing positive for marijuana, despite the worker having a medical marijuana card. The worker had claimed disability discrimination.

The lawsuit is a victory for employers who maintain a zero-tolerance policy towards drug use, even if it's not being done at work.

In the case, *Garcia vs. Tractor Supply Company*, a new employee at a New Mexico company had told the hiring manager during his job interview that he was using marijuana for medical purposes (as allowed by state law) to alleviate his Aids symptoms.

Despite that, he was hired and, like all new hires, he was administered a drug test, which he failed. The next day he was fired in accordance with the company's zero tolerance towards employee drug use.

Shortly thereafter, the employee filed a lawsuit accusing the company of disability discrimination and that under the Americans with Disabilities Act the employer was obliged to accommodate his medical condition by allowing his medical marijuana use.

The judge disagreed and dismissed Garcia's claim.

What you need to know

While this case was in New Mexico, the court's ruling mirrors similar cases in other states with medical marijuana laws or outright legal pot use, including California, Washington, Oregon and Colorado.

In each of these states, the highest court in the jurisdiction ruled that employers did not have to accommodate the medical marijuana usage by job applicants or current employees.

The gist of all these lawsuits and decisions is that even though a state decriminalizes pot for medicinal use, it does not mean that employers have to allow their workers to use it. All of the courts have also cited the fact that marijuana is still illegal under federal law.

Employers, then, can have policies that prohibit its use on the job, or even if an employee or job applicant tests positive for the drug.

But, even if you are located in a state where the law permits you to terminate anyone who fails a drug test, you need to make sure that you are enforcing your policies consistently in order to avoid legal liability.

In the above case, the court sided with Tractor Supply Company because it had enforced its policy consistently by terminating all others who had failed the company drug test. It also found no evidence of disability discrimination on the part of the employer. ❖

Continued from page 1

Insurance Coverage Depends on Reason for Disruption

- Implement a strict password policy and have employees change passwords every 90 days.
- Limit employee access to company data and information, and limit authority to install software to just a few key employees.
- Make sure you are covered by a cyber liability insurance policy.

Covering a business interruption

Insurance coverage will depend on the reason for a disruption to your operations due to a failure of your network, website or cloud service.

If a network goes down because of a fire, for example, rendering the servers inoperable, your property insurance would cover the costs of replacing the servers and a standard business interruption policy would cover lost revenues.

However, if an outage is purely a network issue or due to a cyber attack, then a good cyber insurance program would likely come into play.

Most cyber policies provide an option for covering the costs of business interruption from a network security failure. That includes incidents like DDoS attacks or hackers accessing your network and deleting critical files, or adding malicious code that causes the system to fail.

Some cyber insurance policies will also cover a system failure, such as an "unintentional or unplanned outage" on your network.

Coverage would kick in if the failure was the result of human or system error, or both.

For example, this could include an instance of you installing a new inventory management system and it unexpectedly causes your network or website to crash.

Unfortunately, very few insurers offer this coverage extension now, but as more organizations become more reliant on technology, more products will enter the marketplace.

Cloud risk

But what if a cloud service that hosts all of your important data fails? You could be left holding the bag because most outside vendors often contractually limit their liability for outages.

Under a typical business interruption scenario, if your business is disrupted as a result of a vendor or supplier going down, a contingent business interruption policy would cover it. But, few such policies will cover a cloud failure.

Still, some cyber policies offer this coverage.

So, if a cloud failure would be catastrophic to your operations, talk to us about this option. ❖

WORKERS' COMP

Tech Roots out Fraud, Identifies Problem Claims

WITH DECADES of information in their databases, many insurers have started using those statistics to their advantage to intervene earlier in problem claims and to identify potential fraud.

With years of data to rely on, insurers have identified certain triggers that can indicate that a claim may require additional intervention and more hands-on management.

A predictive modeling program will alert a claims adjuster when it identifies certain parameters or events.

This early identification of problem claims is helping employers and insurers achieve better outcomes for injured workers, as well as save money and time.

As the trend continues, it should help reduce claims costs by eliminating more fraud and also lower the cost of some claims and reduce the time some injured employees are away from work recovering.

Conventional wisdom in workers' comp is that 20% of the claims account for 80% of the losses. Efforts such as early claims reporting, medical case management and return to work have long proved essential for reducing claims.

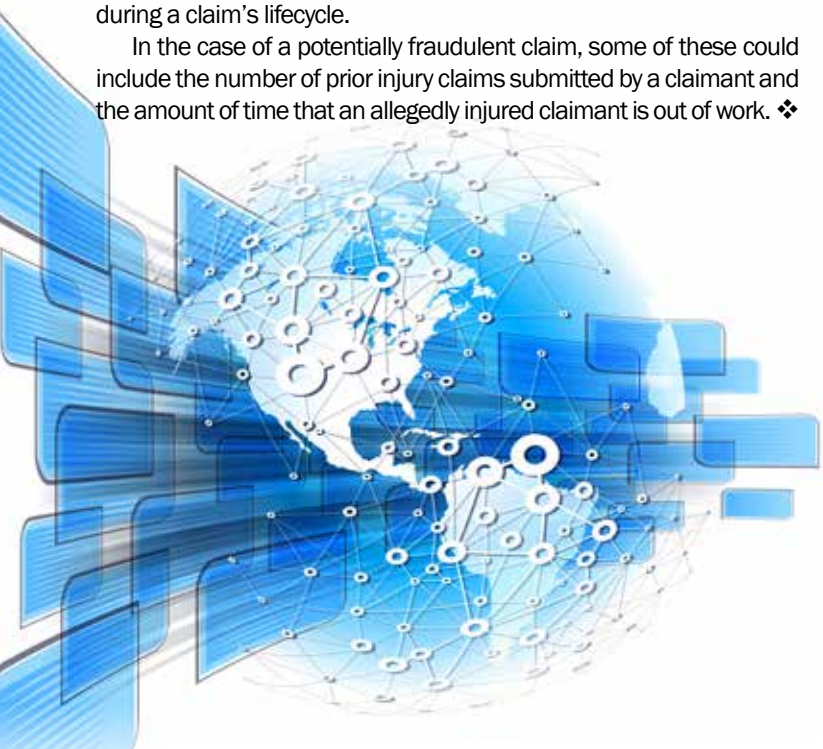
Predictive modeling aims to improve the ability of insurers to identify claims that require early intervention.

Insurance predictive modeling applies statistical techniques and algorithms on insurance and claims data to develop variables that predict the likelihood of a particular situation (like a worker staying off work for longer than average).

While predictive modeling has been successfully used for years by automobile insurers, it's been slower to catch on in workers' comp, particularly because it requires multiple data sets for which data availability can be scarce.

Predictive modeling begins with the first notice of loss and then continues to monitor for certain trigger points and specific actions during a claim's lifecycle.

In the case of a potentially fraudulent claim, some of these could include the number of prior injury claims submitted by a claimant and the amount of time that an allegedly injured claimant is out of work. ❖



Employer tackles medical costs

Supermarket chain Ahold USA, a self-insured employer, started using predictive modeling in early 2012.

Ahold's model uses claim characteristics, medical transaction details, and other data sources to identify factors that are predictive of higher claims costs.

Some of the indicators the company uses include multiple visits to doctors and the use of certain prescription drugs.

The model then prioritizes claims that need special handling and medical case management.

This helps injured employees receive appropriate medical care to reach maximum medical improvement and return to work sooner.

The company's predictive modeling can indicate whether a claim has the propensity to develop adversely.

It can also be used to evaluate the likelihood that a claim will result in litigation.

It may also provide the ability to identify workers' compensation claims with a greater likelihood of surgery. Such tools allow adjusters to develop case strategies at first notice and gain control over the claim as it progresses.

The results for Ahold have been positive, resulting in lower workers' comp expenditures in "low seven digits."

Insurer bird dogs fraud faster

National insurance company Chubb Corp. has been using predictive modeling for both its workers' comp and automobile claims.

At Chubb, predictive modeling begins with the first notice of loss and then continues to monitor for certain trigger points and specific actions during a claim's lifecycle, such as the number of prior injury claims submitted by a claimant and the amount of time that an allegedly injured claimant is out of work.

The model flags claims based on patterns that have historically proven fraudulent and patterns that the claims adjuster may not detect.

If a claim is flagged, the adjuster can investigate further and/or monitor the claim.

If certain warning signs appear, the claim is referred to Chubb's insurer's special investigation unit. At that point the SIU can work with the claims adjuster to investigate further.

Before predictive modeling at Chubb, it could take up to 180 days to spot potentially fraudulent workers' comp claims and assign them to the SIU. Now that number is down to six days.

Also, predictive modeling has led to a significant increase in accepted referrals to the insurer's SIU. As a result, the number of investigation days has decreased, and the company has achieved significant cost savings.

WORKPLACE SAFETY

Protecting Your Workers in the Rain

EMPLOYEES WORKING in the rain face specific hazards, such as poor visibility and wet, slippery surfaces.

When it's wet and windy, potential hazards at a worksite can be exacerbated. Working in the rain can cause slippery surfaces and limited visibility.

It's also riskier to use heavy equipment in the rain, particularly when moving heavy loads, putting workers on the ground – and even the public – in danger.

However, steps can be taken to mitigate such hazards.

It's imperative that you as an employer ensure your employees' safety, especially during this heavy year for rain.

When working in the rain, train your employees to:

- **Move cautiously** – While workers may be tempted to move fast in the rain to avoid getting wet, this can be dangerous, especially on slippery surfaces. If anything, they should work more slowly and deliberately in all of their tasks.
- **Use the correct equipment** – If workers must use electrical tools or equipment, they need to check that they are specifically rated for outdoors. Also, the tools should have textured, no-slip grips and handles.
- **Don proper footwear** – Workers should wear footwear with heavy treads that can reduce the chances of slipping.
- **Remember rain gear** – Proper rain gear includes rain pants and a raincoat. The best clothing is ventilated to help your workers stay comfortable. If it's cold and rainy, they should also wear wool or synthetic materials that can stay warm even when wet.
- **Wear non-slip gloves** – Workers should wear gloves that provide a sticky grip even when wet. Gloves should be snug and long enough for a jacket sleeve to prevent water from entering.
- **Keep vision clear** – Workers who wear glasses (if they must wear goggles for certain jobs) should apply anti-fog spray to them. It's also advisable to wear a hat to keep rain from their eyes. They shouldn't use headgear that narrows their field of vision.
- **Work in proper lighting** – When working at night, workers should make sure lighting is adequate and the lights used are rated for outdoor use.
- **Ensure visibility** – When it's raining, visibility decreases and it's easy for motorists and machine operators to have trouble seeing properly. Workers should wear high-visibility clothing, especially in areas with vehicle traffic and heavy machinery. Don't wear rain gear or vests that have become dull or are no longer reflective.

Cold stress

When it rains, it's often cold, too – and wet clothing can exacerbate the cold.

Employees working outdoors for prolonged periods of time when it's cold must be protected from cold stress. Cold stress can cause frostbite, hypothermia and trench foot.

OSHA advises that cold stress is not limited to freezing temperatures, and can occur in outdoor temperatures in the 50-degree Fahrenheit range when rain and wind are present.

OSHA requires addressing this hazard by using protective clothing, in particular the use of layers with an outer material that protects against wind and rain.

Although OSHA generally requires employers to pay for their workers' protective equipment, employers are not required to pay for ordinary clothing such as raincoats.

Heavy-work dangers

Rain makes operating cranes, derricks and hoists more dangerous as well, particularly when moving large and heavy objects. Heavy rain combined with wind speed can make loads difficult to control.

Also, if a rainstorm is accompanied by lightning, equipment such as a crane can become a lightning rod.

If you feel you cannot adequately protect your workers during a storm, you should not conduct operations in the rain. ❖