HEFFERNAN INSURANCE BROKERS
Because You're Different

News You Can Use

October 2016 Volume 4, Issue 12

CYBER SECURITY

The True Costs of Ransomware Go Beyond Ransom

ONE OF the least understood cyber threats to businesses is ransomware, which hackers use to shut down an organization's computer system until the victim pays a ransom to unlock it.

While most organizations focus on the cost of the ransom, which is often less than $2,000, the costlier damage is to the company's operations, which can be hampered or completely shut down after their systems are rendered unusable.

Ransomware is one of the fastest-growing cyber threats and attacks are expected to grow 300% in 2016 from the year prior, making it vital for your organization to have in place systems to reduce the chances of becoming victimized.

Ransomware typically enters computer systems after an employee clicks on a link in a rogue e-mail, which allows the malicious code entry. Eventually it can seal off your database, locking out all users and making all or some of the data inaccessible. After it has frozen the systems, it will demand a ransom to unlock it.

The full damage

According to the FBI, there were 2,400 ransomware complaints in 2015, resulting in total estimated losses of more than $24 million with the average ransom demand being $10,000. But it's believed that most attacks go unreported.

Ransomware typically targets your most important data, but sometimes it just makes your entire system unusable. It may also lock down your marketing materials, payroll data, intellectual property, financial transactions and health records.

Ransomware criminals who are not paid will often destroy the decryption key, leaving affected companies in a more serious bind.

If you're lucky, a ransomware attack may only be confined to one server or computer. But if it hits the right servers, it can spread throughout your organization to all users and, if you are connected with vendors or partners, it can even spread to their systems.

Controlling risk

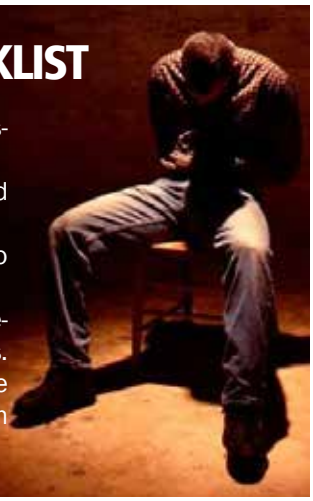
CFO magazine recommends that you do the following to reduce the risk of being hit by ransomware:

- Train and educate personnel on an ongoing basis.
- Specifically address and plan for ransomware in your disaster recovery and business continuity plans, including testing of those plans.
- Ensure that all anti-virus and other security software is properly updated. This software will detect and eliminate many forms of ransomware.
- Engage a third-party expert security vendor to assess your organization's systems and procedures.

See 'Cyber' on page 2

RANSOMWARE RESPONSE CHECKLIST

- Identify and isolate infected and potentially infected systems.
- Disable shared network drives connected to the infected systems.
- Consider suspending regular backups of those systems to prevent the virus from spreading further.
- Engage an information security consulting firm that specializes in assessing and mitigating these sorts of attacks.
- Send out a memo to all your staff warning them of the infiltration and to not open e-mail and attachments from suspicious sources.



Contact Us

HEFFERNAN INSURANCE BROKERS

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

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

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

H.R. ALERT

Countdown to New Overtime Exemption Rules

IF YOU have not yet done so, now is the time to start preparing all of your accounting and payroll systems for the onset of the Department of Labor's new overtime exemption rules.

And California employers have to pay special attention going forward because in a few years the state threshold will surpass the national threshold that takes effect Dec. 1.

The regulations change the salary level that must be met before an employee can be exempt from overtime if they satisfy the "duty requirement," meaning they have to be engaged in certain white collar jobs.

But while the rules are generally straightforward, employers in California will have a different standard to meet in the years to come and compliance will become trickier.

Under the DOL's final rule, starting Dec. 1, employers will be required to pay overtime to full-time employees who earn less than $913 per week ($47,476 per year), regardless of their duties. Employees who earn more than that and have white collar, management level jobs would be exempt from overtime.

This new threshold is more than double the current $455 per week ($23,660 annually). Currently, the salary threshold for the overtime exemption for white collar workers in California is $41,600 a year, or $3,466.67 per month, but it will rise to the federal level on Dec. 1

California's overtime exemption level is based on twice the state minimum wage, which is set to substantially increase in the coming years, hitting $12 an hour in 2019 and $15 an hour by 2022. After that, it will continue to rise based on inflation.

For example, on Jan. 1, 2019, when California's minimum wage hits $12 per hour, the overtime-exempt threshold for California employers will be $49,920. That's $2,444 higher than the impending federal threshold.

Do the math for 2022, and the California threshold will hit $62,400.

The federal minimum salary threshold will also be automatically updated every three years. The first update will be in 2020, and a White House projection predicts the salary threshold will rise to $51,000 at that time.

Duties test

California also has a different duties test than that of the Fair Labor Standards Act.

The federal duties test for white collar exemptions requires exempt employees to be "primarily engaged" in certain duties, like managing people and making decisions independently.

In California, an exempt employee must spend more than half of his or her time engaged in exempt work. ❖

Get current now

Here is a checklist of action items that you should address immediately:

- Check whether your salaried employees satisfy the duties and salaries components of the FLSA white collar exemptions (or California law).
- Identify all of the positions that will require reclassification under the new rule and decide whether it is worth it to increase someone's salary.
- Analyze the financial impact of reclassifying employees as nonexempt.
- Consider reassigning certain tasks to reduce the effects of the rule.
- Make plans to conduct reviews regularly – like every three years for federal law compliance, or more frequently in California ahead of minimum wage changes.

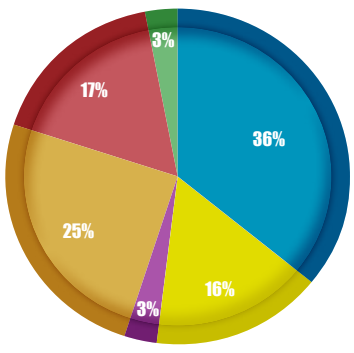
Continued from page 1

Cyber Insurance Can Pay for Ransomware Fallout

Insurance

Cyber insurance can pay for the effects of a ransomware attack. Depending on the insurer, some policies will pay the ransom, while others expressly exclude it, citing the "moral hazard" of such coverage.

If you are concerned about the damage an attack could inflict on your organization, call us to discuss your cyber insurance options. ❖



RANSOMWARE BUSINESS INTERRUPTION LOSSES

- Corporate loss of business income or services
- Corporate loss of digital assets
- Corporate loss of financial assets
- Breach of personally identifiable information
- Breach of personal financial identity
- Breach of personal health information

WORKERS' COMP

How Three Firms Reduced Their Claims Costs

WE'VE TOLD you often in these pages about workplace safety and claims management techniques, but sometimes it's good to learn from the experiences of other employers.

The *National Underwriter* insurance trade publication recently profiled three companies that had reduced their workers' comp costs using a combination of claims management and safety initiatives.

You can use their experience to apply similar programs.

SMS Holdings: Get employees involved

This housekeeping and maintenance service provider did not roll out a one-size-fits-all approach to safety at is multiple locations and asked front line staff and their supervisors to come up with programs to enhance safety at each work site. Here are the main changes:

- It created safety committees at each of its locations that hold pre-shift safety huddles. Site managers host weekly safety talks with employees that address hazards at the site and near misses.
- It started a tracking program that provides a forum for managers to exchange ideas on how injuries could have been prevented.
- It revised its injury reporting system, standardized claims instructions and forms and provided a claims checklist for managers.
- It gives injured workers a packet that outlines the process for handling claims and includes all forms and contact information.

THE RESULTS

❒ Claims litigation rate fell 40%
❒ Claims dropped more than 14%
❒ Lost-time claims plunged 52%

Seaboard Foods: Quick medical response cuts costs

After noting a strong uptick in claims, this self-insured, 5,000-employee pork producer took action:

- It started working more closely with its third-party administrator, which handles its workers' comp claims, to mine the company's injury claims for data.
- It ensures that workers receive the right specialized medical care at the time of injury, even if that means that the employee sees a specialist in another town.
- It started contracting with new service providers – like physical therapy and pharmacy management firms – that could demonstrate through data how they are able to reduce costs.
- It started holding quarterly meetings with its senior leadership, workers' comp team, third-party administrator and workers' compensation attorney to review claims. They set goals and objectives for closing claims as early as possible and identifying particular claims that the company would try to close prior to the next quarter.
- It started conducting job-demand analyses to identify how employees get hurt doing certain tasks, and then evaluating workers to make sure they are fit for the work they've been assigned.

THE RESULTS

❒ Claims fell by 46%
❒ Claims costs dropped 69%
❒ Injured workers return to work faster

Stater Bros. Markets: Refocus on workplace safety

This supermarket chain started a new program focused on education and injury prevention for all of its employees, be they cashiers or workers at its California warehouse and distribution center.

- It requires workers who use knives to wear a chain-link metal mesh glove on the hand opposite the one wielding the knife.
- It reviewed the clinics its injured workers are sent to, selecting facilities based on level of customer service and cleanliness.
- It started a program teaching staff and low-level managers at each store on injury prevention, focusing mainly on avoiding sprains and strains – the most common injuries in its stores.
- It makes physical therapists available at its corporate campus to help warehouse staff with taping, wrapping and icing parts of the body to help them do their jobs or recover after a shift.
- It conducted a claims review to identify problematic prescription patterns. It met with the health care providers and worked with pain-management doctors to find alternatives to prescribing so many drugs, which employees often are not taking.

THE RESULTS

❒ Cutting injuries were reduced from 200 a year to none
❒ Prescription drug costs fell $1 million over two years

RISK MANAGEMENT

Review, Update Your Business Continuity Plans

WE OFTEN urge you to have a risk management plan in place so that you are prepared for the many eventualities that can affect your business.

Your risk management plan should be part of a larger business continuity plan for keeping your organization going during periods of disruptions that are both large and small.

The plan should be broad to cover prevention and response, and that can only be done with input from representatives of all your firm's divisions.

Companies can spend considerable time putting together a risk management plan that is unique to their workplace and operations. But, after they have created and implemented their plan, many businesses fail to evaluate and update it on a regular basis.

You will need to test, evaluate and update your risk management and business continuity plans regularly because risks can change as your business, your industry and the environment you operate in also change.

A prime example of a new risk is the cyber threat that continues to grow in significance, having cost many businesses millions of dollars in response, remediation and notification costs. If you have not included this eventuality in your business continuity plans, you should do so.

If you set aside time once or twice a year to review your plans, you can identify new risks and monitor the effectiveness of your current risk management strategies. This gives you an opportunity to modify or enhance your plan in response to those emerging or newly identified threats.

THE BUSINESS CONTINUITY PLAN

Besides identifying and trying to mitigate for risks that you identify, your risk management plan should be part of a broader business continuity plan that includes strategies for responding to and recovering from incidents if they do happen:

Prevention – This is essentially the risk management part of the plan, which is to prevent problems from occurring in the first place.

Preparedness – This should be the fruits of your risk management plan, requiring to you have plans and resources in place to respond and recover from an incident. You should conduct a business impact analysis that identifies all of the resources, personnel and equipment critical to keeping your business running.

Your plan should identify external stakeholders, the skills and knowledge necessary to run your business and how long your business can survive without performing these tasks.

Response – This part of the plan should cover what you do following an incident, such as containing, controlling and minimizing the effects. This should include details on when the plan would be activated, assembling an emergency kit, having evacuation procedures in place and a communication plan to implement during an event.

Recovery – After the initial response to an incident you will want to ramp up to full operations again as quickly as possible. You need to map out strategies to recover your business activities in the quickest possible time. That entails a description of key resources, equipment and staff required to recover your operations – and a time objective.

As you did when you created your original plans, you should involve personnel from your various departments and also consider inviting key vendors or customers to the planning sessions. This will help bring different perspectives to the table, resulting in a more comprehensive overall plan.

While you may be able to predict and deal with a number of potential risks, there will be some that are unexpected or impossible to plan for.

That's why the last two parts of your business continuity plan – incident response and recovery – are important, as they can be used after both foreseeable and unforeseeable events.

A business continuity plan is a blueprint for how your business will recover or restore critical activities after a crisis. ❖