NEWS YOU CAN USE
VITAS INSURANCE AGENCY
April 2014, Volume 5, Issue 2

DATA SECURITY

California Is Nation's Top Cyber Crime Target

CALIFORNIA IS a major target of cyber crime in the U.S., accounting for one in six hacks into major computer systems in the country, according to a new report by the state Attorney General's office.

While the damages are in the billions nationwide from hacking attacks mostly on businesses, California by a large margin tops all states in the number of hacked systems, the number of computer systems infected by malware, the number of victims of Internet crimes, the losses suffered as a result of those crimes, and the number of victims of identity fraud, according to the report.

Also, because of the outsized role new technologies play in its information-based economy, California is particularly vulnerable when its networks become infected and its intellectual property is stolen.

In 2012, the Privacy Rights Clearinghouse recorded at least 331 breaches in the U.S. caused by international criminals who were purposefully trying to compromise databases or networks. California accounted for 17% of those breaches which, in turn, contributed to putting at risk the sensitive personal information of at least 2.5 million Californians that year, according to the report.

Between 2009 and 2012, the number of intentional breaches in the U.S. jumped by 280%, but during that same period the number of breaches in California shot up 560%.

The rapid increase in international breaches both in the state and nationwide should be cause for concern for any business that has an online presence, but particularly for those that have sensitive customer information online, like ID information and credit cards.

Cyber security best practices

Strong passwords – Use strong passwords and change them regularly. Passwords are the first line of defense in preventing unauthorized access to any computer. The more complex, the better, with a combination of characters, letters and numbers.

Install and maintain anti-virus software – The primary way that attackers compromise computers in the small office is through viruses and similar code that exploits vulnerabilities on the machine. You should train your staff on how to recognize a computer virus infection.

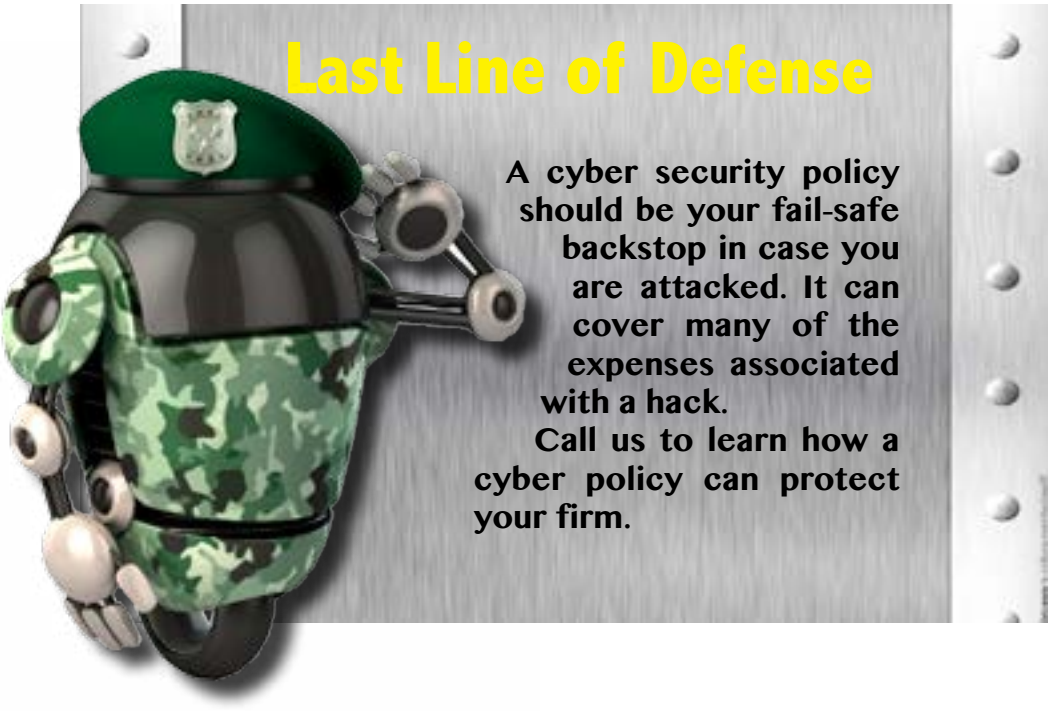
Use a firewall – Unless you have a database that is totally disconnected from the Internet, it should have a firewall to protect against intrusions and threats from outside sources. While anti-virus software will help to find and destroy malicious software that has already entered, a firewall's job is to prevent intruders from entering in the first place.

Secure socket layer – If you are handling credit card transactions, make sure that your payment system includes a secure socket layer to encrypt all of the important data of each customer.

Control physical access – Not only must assets like files and information be secured, the devices that your employee use must also be safe from unauthorized access. The single most common way that protected data is compromised is through the loss of devices themselves, whether through theft or accidentally.

Limit network access – Limit access to your

(See 'Security' on page 2)



CONTACT US

VITAS INSURANCE AGENCY

If you have a question about any of the articles in this newsletter or coverage questions, contact your broker at one of our offices.

Vitas Insurance Agency
200 Auburn Folsom Road, Suite 300
Auburn, CA 95603
Contact: info@vitasinsurance.com
License Number 0D87937

WORKPLACE SAFETY

Summer's Coming, Protect Your Outdoor Workers!

AS SUMMER approaches employers with outside workers need to make sure that they are in compliance with Cal/OSHA's heat illness prevention standard to protect their employees, and also to avoid being cited.

Over the years the heat illness standard has evolved as more is learned about how heat illness works. The following covers the major elements of the standard.

Access to water

- Locate the water containers as close as practicable given the working conditions and layout of the worksite.
- Keep it readily accessible, move it with the workers!
- Encourage the frequent drinking of water.
- Remind workers not to wait until they are thirsty.

Shade up at 85 degrees

- When temperatures reach 85, you must have and maintain one or more areas of shade at all times, when employees are present.
- Locate the shade as close as practical to the area where employees are working.
- Provide enough shade to accommodate at least 25% of the employees on the shift at any one time. However, retain the ability to permit access to all workers that request it at all times.

High-heat procedures

When the temperature equals or exceeds 95 degrees:

- Ensure effective communication.
- Observe employees for alertness and signs and symptoms of heat illness.
- Give more frequent reminders to drink plenty of water.
- Closely supervise new employees, for the first 14 days.

Training

Ensure all employees and supervisors are trained before beginning work that should reasonably be anticipated to result in a heat illness. Make sure all employees and supervisors are trained in:

- The environmental and personal risk factors for heat illness, as well as the added burden of heat load on the body
- Your company's heat illness prevention procedures
- Importance of frequent consumption of small quantities of water
- Types of heat illness, common signs and symptoms
- Importance of acclimatization
- Reporting signs or symptoms of heat illness to a supervisor
- Procedures for responding to possible heat illness
- Procedures to follow when contacting emergency medical services, providing first aid, and if necessary transporting employees.

Written procedures

- Integrate your procedures into the IIPP.
- Maintain the procedures on site or close to the site, so that they can be made available to employees and Cal/OSHA inspectors.
- You can find sample procedures here: *www.dir.ca.gov/dosh/dosh_publications/ESPHIP.pdf* ❖

(Continued from page 1)

Establish a Security Culture throughout Your Organization

most important information to only a few individuals in your organization.

Plan for the unexpected – Natural or man-made disasters can strike at any time.

Important health care records and other vital assets must be protected against loss.

There are two key parts to this practice: creating backups and having a sound recovery plan.

Configuration management – New computers and software packages are delivered with a dizzying array of options, but little guidance on how to configure them so that the system is secure.

In the face of this complexity, it can be difficult to know which options to permit and which to turn off. Here are some rules of thumb:

- Uninstall any software application that is not essential to running your business (e.g., games, IM clients, photo-sharing tools).
- Do not simply accept defaults or standard configurations when installing software. Step through each option, understand the choices, and obtain technical assistance where necessary.
- Disable remote file sharing and remote printing within the operating system configuration. Allowing these could result in the accidental sharing or printing of files to locations where unauthorized individuals could view them.

Protect mobile devices – Laptops, smart phones and portable storage media are even more vulnerable to hacking, making it easier for hackers to gain entrance to your company data. Because of their mobility, these devices are easy to lose and vulnerable to theft. Make sure they are protected, too.

Establish a security culture – None of the above measures can be effective unless your staff is willing and able to implement them, and you enforce policies that require these safeguards to be used. In short, you must instill and support a security-minded culture. ❖

PAPER TRAIL

Pay Attention to ACA Reporting Requirements

THE ADMINISTRATIVE burden on businesses is increasing as a result of the Affordable Care Act, requiring you to keep meticulous records that you may not be accustomed to.

Specifically, there are three main ACA reporting requirements that employers need to be aware of and prepare their accounting department for. The first one has already taken effect, but the other two were postponed until 2015.

The following sections cover each of the three ACA reporting requirements in detail.

W-2 and wage and tax statements

The ACA added a new section to the tax code in terms of what needs to be reported on an employee's W-2 form, as well as pay stubs.

The rules took effect with W-2 forms issued for the 2012 tax year, adding a new box: 12DD, which must specify the aggregate cost of applicable employer-sponsored coverage.

The Section 6051(a)(14) reporting mandate applies to all employers that issue at least 250 W-2 forms annually. Employers will have to send in new Box 12DD data prior to Feb. 1 every year. The Box 12DD amount must include both the portion of the health benefits total paid by the employer and the portion paid by the employee, according to the implementing regulations.

If the health plan is insured, the employer can use the premium charged by the insurer for that employee's coverage (as applicable to the employee) as the reportable cost.

This Box 12DD total should not include contributions to health savings accounts or most contributions to flexible spending arrangements (FSAs). The Box 12DD total should include spending on:

- Major medical coverage.
- A health FSA for the plan year in excess of an employee's cafeteria plan salary reduction for all qualified benefits.
- A hospital indemnity or specified illness arrangement (either insured or self-funded), paid through a pretax salary reduction program or by the employer.
- Domestic partner coverage included in gross income.

This reporting, while required, is informational only.

Reporting who is covered

Under Section 6055 (the rules are only proposed and not final), plan sponsors must report to the IRS who is covered by the plans and the months in which they were covered. Plan sponsors must also provide this information to employees enrolled in their plans.

Plan sponsors must report:

- The name, address and social security number (SSN) of the primary insured, and the name and SSN for each other individual obtaining coverage under the policy.
- The dates during which the individual was covered under minimum essential coverage during the calendar year.
- Any other information as the IRS may require.

Detailed plan reporting

Under Code Section 6056 (regulations are as yet only proposed and not finalized), applicable large employers must report to the IRS, and provide to affected full-time employees, information that includes:

- The employer's contact information;
- Whether the company offered minimum essential coverage to full-time employees and their dependents;
- The months during which coverage was available;
- The monthly cost to employees for the lowest self-only minimum essential coverage;
- The number of full-time employees each month of the year;
- Information about each full-time employee and the months they were covered under the plan.

Simplified reporting?

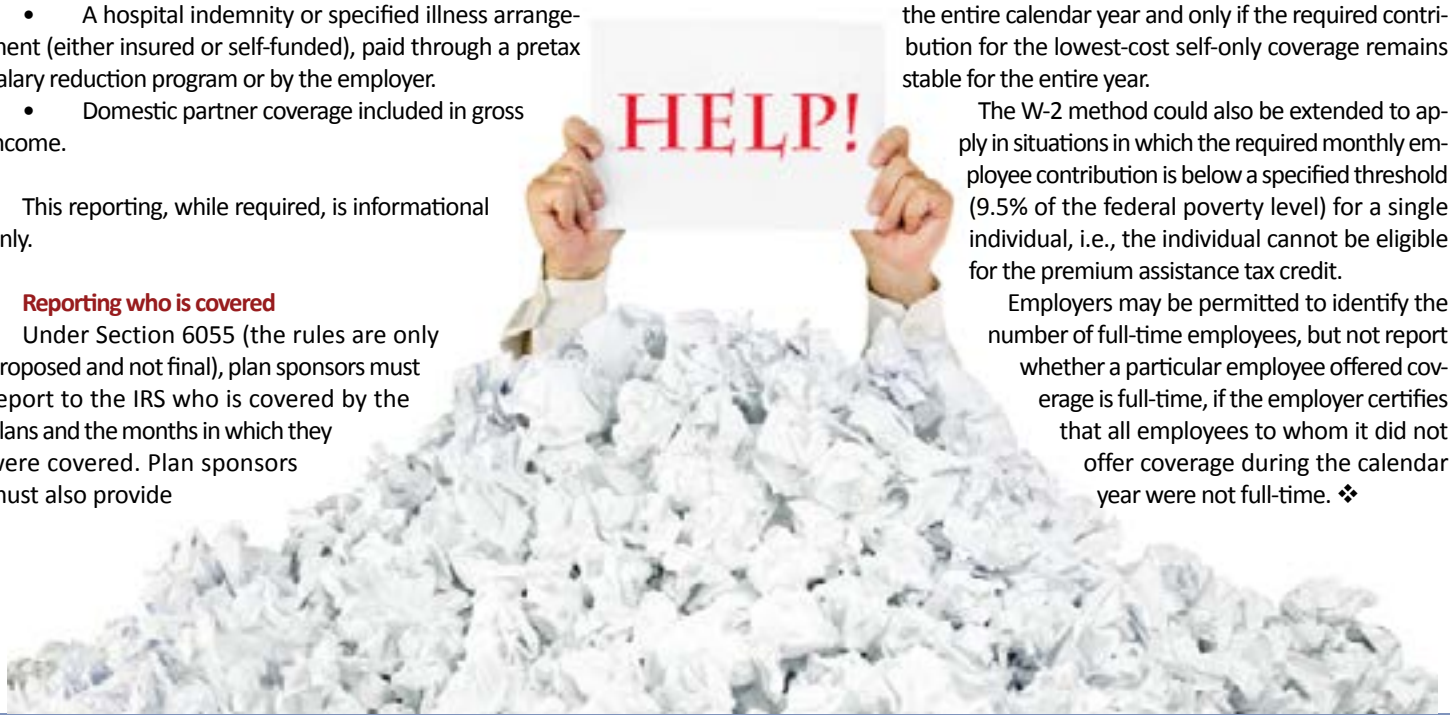
The cost of compiling, processing and distributing the reports will likely be substantial for many employers. The Department of Treasury did make some suggestions on how reporting may be simplified.

For example, employers might be permitted to report coverage on W-2 forms, rather than requiring a separate return under Section 6055 and furnishing separate employee statements.

However, this approach could be used only for workers employed for the entire calendar year and only if the required contribution for the lowest-cost self-only coverage remains stable for the entire year.

The W-2 method could also be extended to apply in situations in which the required monthly employee contribution is below a specified threshold (9.5% of the federal poverty level) for a single individual, i.e., the individual cannot be eligible for the premium assistance tax credit.

Employers may be permitted to identify the number of full-time employees, but not report whether a particular employee offered coverage is full-time, if the employer certifies that all employees to whom it did not offer coverage during the calendar year were not full-time. ❖



WORKERS' COMP

When You Can and Can't Discipline a Claimant

HERE'S A SITUATION you may want to avoid: disciplining workers who report workplace injuries. It's against state workers' comp laws and could land you in hot water with OSHA.

That's what happened recently to Ohio Bell Telephone Co., which the U.S. Department of Labor sued, accusing the company of violating whistleblower provisions of the Occupational Safety and Health Act of 1970 after it disciplined 13 workers who had reported workplace injuries.

The case illustrates what not to do if you have employees who file workers' comp claims, even if you suspect that they may be fraudulent.

The lawsuit, filed in U.S. District Court in Cleveland against Cleveland-based Ohio Bell, accuses the phone company of issuing one- to three-day suspensions and/or issuing written disciplinary warnings against the workers.

The lawsuit cites the case of one worker who injured his back, shoulder and neck in January 2013, while loading boxes into his work vehicle at Ohio Bell. He sought medical treatment on Jan. 18, and was released back to work on Jan. 31, 2013.

Ohio Bell determined that he had violated its ergonomics policy and issued him a written disciplinary warning and assessed a one-day suspension, which he served on Feb. 12, 2013, according to the lawsuit.

The suit charges the company with violating OSHA's whistleblower provisions.Besides OSHA's whistleblower protections, most states have laws that prohibit employers from disciplining workers for filing workers' comp claims.

Depending on the state, the complaint can be filed inside or outside the workers' comp system and, in the case of the latter, it can open up the employer to punitive and compensatory damages.

In California, the effective law is Section 132(a) of the Labor Code, which makes it a misdemeanor for an employer to discriminate in any way, including discharge or threat of discharge, against an employee who has filed or is thinking about filing a workers' comp claim or an employee who has received a workers' compensation award. The employee who has been discriminated against is entitled to a maximum penalty of $10,000. ❖

The Workplace Discipline Playbook

Administering discipline against someone who has filed a workers' comp claim can be tricky, but you should be protected if you have good cause, treat employees consistently, and have good documentation.

Good cause — To test whether good cause applies, you should balance management discretion with fairness to the employee.

One aspect of proving there was good cause can be to show that the behavior that spurred you to consider disciplinary measures was clearly against company policy. For example, is the infraction described in your employee handbook?

Consistent application — Even-handed enforcement of the rules is critical to ensure that one employee is not punished more than others. Failing to be even-handed can make it seem as though enforcement of the rules is only a pretext for the real reason for discipline: retaliation for the workers' compensation claim.

Consistent application is important. For example, even if the rule is in the handbook, the employee could argue that the rule was broken by everyone and enforced selectively against him. Alternatively, if the rule was not in the handbook, it could be argued that it was made specifically for him as a means of discriminating against him.

Documentation – The golden rule of disciplining employees is documentation, regardless of whether they have a filed workers' comp claim. Documentation is your evidence to back up the need for discipline. If you don't have any evidence other than the supervisor's observations – even if the supervisor says that the misconduct has been consistent – do not proceed with terminating the employee.

To start the documentation process, advise the employee of the unacceptable behavior and give them an opportunity to improve. Document what you have told them and have them sign the agreement that they will improve their behavior.

If they don't, then you've got the start of documentation to be able to take further action later. Again, consistent enforcement of the rules is key.

Document infractions of all employees and supervisors – not just those of the employee in question.