Whitman Samuelson
INSURANCE SERVICES, INC.
• Since 1931 •

The Insurance Watch

Sept. 2011 Volume 1 Issue 2

Internet Sales

Make Sure to Protect Your Clients' Data

IF YOUR company conducts any type of activity — particularly sales on the Internet — that requires you to keep business and consumer credit information, you need to take steps to protect your clients' data from theft.

And just because you operate a small or mid-sized business does not make you immune. While highly publicized hacking events at Sony Corp. and CitiBank that exposed the data of thousands of consumers were shocking, a new study indicates that hackers are shifting focus to smaller companies, which have fewer defenses in place than their corporate counterparts.

In 2010, the U.S. Secret Service and Verizon Communications Inc.'s forensic analysis unit, which investigates attacks, responded to a combined 761 data breaches, up from 141 in 2009. Of those, 482, or 63%, were at firms with 100 or fewer employees, according to the *Wall Street Journal*. And Visa Inc. estimates that about 95% of the credit-card data breaches it discovers are on its smallest business customers.

If you are a retailer, your data banks will certainly have customer credit-card information.

In some businesess you may have more data, and in many cases you may have much more — like names and addresses, Social Security numbers, credit-card numbers, or other account numbers — about your customers, employees, business partners, students or patients. If this information falls into the wrong hands, it could put these individuals at risk for identity theft.

A 2010 survey of small and medium-sized retailers in the U.S. by the National Retail Federation and First Data Corp. found that 64% believed their businesses weren't vulnerable to card data theft and only 49% had assessed their security safeguards.

One of the most common styles of attack on small businesses targets credit-card information that a hacker can sell or use to make fraudulent purchases. To gird against this, the major credit-card companies in 2006 formed an industry group called the Payment Card Industry Security Standards Council, which establishes minimum technical protections for businesses that accept credit cards.

While credit-card companies require all businesses that accept their cards to comply with those standards, known as PCI, they have few measures to enforce them for small businesses. Bob Russo, general manager of the PCI Council, says many small businesses neglect basic security measures such as changing default passwords.

Visa and the PCI Council recommend the following steps, broken down into three areas:

Eliminating prohibited data

- Small businesses that use commercially available point of sale (POS) systems or payment software should contact their vendors to determine whether the systems they use store prohibited data after transaction authorization.
- In particular, ask your POS or payment software vendor (or reseller) to confirm that your current software version does not store magnetic stripe data, or PINs. If it does, these data elements must be removed, as well as any historical data that has been stored in database or log files.

Protecting stored data

- Encrypt or truncate your data. Small businesses should evaluate whether they must retain full account numbers after a transaction has been authorized.

See 'Encrypt' on page 2

CONTACT US

Whitman Samuelson
INSURANCE SERVICES, INC.

If you have any questions regarding any of these articles or have a coverage question, please contact us.

1012 Clegg Court
Petaluma, CA 94954
Office: 707.794.8701
Fax: 707.794.8707
E-mail: info@whitman-insurance.com
License No.: 0273555

Computer Vision Syndrome

The New Occupational Injury Threat

COMPUTER VISION syndrome (CVS) is more common than carpal tunnel syndrome and other musculoskeletal disorders, according to a recent article in *HR News*,, a trade publication.

According to the American Optometric Association, CVS is characterized by visual symptoms resulting from interaction with a computer display or its environment. In most cases, symptoms occur because the visual demands of the task exceed the visual abilities of the individual to comfortably perform the task.

Symptoms of CVS are eyestrain and fatigue, dry eyes, headaches and neck and shoulder pain.

The association notes that video-display-terminal (VDT)-related vision problems are at least as significant a health concern as the musculoskeletal disorders, such as carpal tunnel syndrome, that receive more attention.

"The vision problems experienced by VDT workers are varied and are difficult to grasp and understand by those who don't specialize in vision," the optometric association stated in the report. "The misunderstanding may also be the result of unfounded reports of cataracts caused by VDTs, exaggerated manufacturer claims about the need for UV and other radiation protections, and misleading statements about the effects of specialty tinted and coated lenses (e.g., computer glasses) among other products."

In most cases, CVS is treatable and modifications to the workplace and regular practices can help. According to VSP VisionCare, an eye-care insurance company, some simple steps to combat CVS include:

- **Keep blinking**. It washes your eyes in natural tears.
- **Remember 20-20-20.** Every 20 minutes, spend 20 seconds looking at something 20 feet away, minimum.
- **Get the right light.** Good lighting is healthy for your eyes. Start by keeping bright lighting overhead to a minimum. Keep your desk lamp shining on your desk, not you. Keep window light off to the side, rather than in front or behind you. Use blinds and get a glare screen. Position the screen to reduce reflections from windows or overhead lights.

- **Monitor your monitor.** Keep it at least 24 inches from your eyes. The center of the screen should be about 4 to 6 inches below your eyes. Also, make sure it's big enough and with just the right brightness and contrast. Adjust the screen so you look at it slightly downward and are about 24 to 28 inches away. Adjust the screen settings to where they are comfortable — contract polarity, resolution, flicker, etc.
- **Wear those computer specs.** Your doctor can prescribe a pair of glasses just for seeing the computer screen well. If necessary, wear the appropriate corrective lenses while at the computer. ❖

Continued from page 1

Encrypt Account Numbers Sent on Public Networks

In many cases, you may be able to fulfill your business requirements on some or all of your systems by retaining only a truncated portion of the account number, such as the first six and last four digits.

- Account numbers transmitted over public networks, such as the Internet or wireless, must be encrypted during transmission using technology such as SSL.
- Install and maintain a firewall to protect data.

Securing the environment

- Replace missing or outdated security patches. Many vendors offer automated alerts that provide prompt notification to their clients. Some vendors also provide automated patching mechanisms. If a patch cannot be applied immediately, other controls to reduce this risk should be implemented, and monitoring of all affected systems should be increased. Small businesses should establish software upgrade policies and procedures to ensure patches are reviewed and installed in a timely manner.
- Check your settings and passwords. Hardware and software products come packaged from vendors with preset passwords and settings. Any default or blank settings and passwords should be changed prior to deployment. In addition, passwords should comply with current industry standards for storing passwords.
- Assign a unique ID to each person with computer access.
- Your business policies should be designed to prevent fraud scams involving collusive employees. As part of this, physical access to information, whether it resides in a computer or a file drawer, should be restricted. Only those employees with a business need should be permitted access. Whenever possible, account numbers should be encrypted or scrambled during transaction processing.
- Unauthorized electronic equipment — such as personal laptop computers — that can be used to steal or replicate account information, should not be allowed in the workplace.
- Track and monitor all access to network resources and cardholder data, regularly test your systems and processes and maintain a policy that addresses information security.

Also, Visa International has issued a guide for protecting credit-card data. It can be found here: *http://usa.visa.com/download/merchants/visa_data_fraud_090707.pdf* ❖

Workplace Safety

Do You Have an Emergency Action Plan?

ALMOST EVERY business is required to have an emergency action plan. If fire extinguishers are required or provided in your workplace, and if anyone will be evacuating during a fire or other emergency, Cal/OSHA requires that you have an EAP.

In most circumstances, immediate evacuation is the best policy, especially if professional firefighting services are available to respond quickly. There may be situations where employee firefighting is warranted to give other workers time to escape, or to prevent danger to others by spread of a fire. In this case, you, as the employer, are still required to have an EAP.

An EAP is a written document required by particular Cal/OSHA standards. The purpose of an EAP is to facilitate and organize employer and employee actions during workplace emergencies. Well-developed emergency plans and proper employee training (such that employees understand their roles and responsibilities when executing the plan) will result in fewer and less severe employee injuries and less structural damage to the facility during emergencies. A poorly prepared plan likely will lead to a disorganized evacuation or emergency response, resulting in confusion, injury and property damage.

Putting together a comprehensive emergency action plan that deals with those issues specific to your worksite is not difficult. It involves taking what you learn from conducting a workplace evaluation and describing how employees will respond to different types of emergencies, taking into account your specific worksite layout, structural features and emergency systems.

Most organizations find it beneficial to include a diverse group of representatives (management and employees) in this planning process and to meet frequently to review progress and allocate development tasks. The commitment and support of all employees is critical to the plan's success in the event of an emergency; so ask staff for their help in establishing and implementing your emergency action plan. For smaller organizations, the plan does not need to be written and may be communicated orally if there are 10 or fewer employees.

At a minimum, the plan must include but is not limited to the following elements:

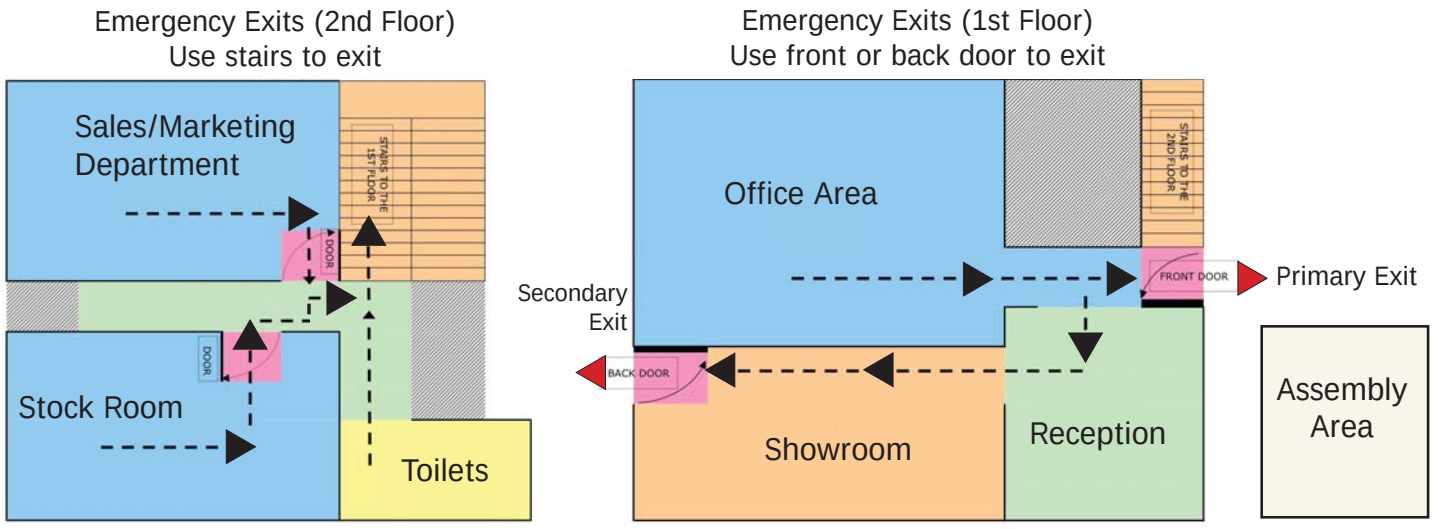
- Means of reporting fires and other emergencies
- Evacuation procedures and emergency escape route assignments
- Procedures to be followed by employees who remain to operate critical plant operations before they evacuate
- Procedures to account for all employees after an emergency evacuation has been completed
- Rescue and medical duties for those employees who are to perform them
- Names or job titles of persons who can be contacted for further information or explanation of duties under the plan

Although they are not specifically required by OSHA, you may find it helpful to include the following in your plan:

- A description of the alarm system to be used to notify employees (including disabled employees) to evacuate and/or take other actions. The alarms used for different actions should be distinctive and might include horn blasts, sirens, or even public address systems.
- The site of an alternative communications center to be used in the event of a fire or explosion; and
- A secure on- or offsite location to store originals or duplicate copies of accounting records, legal documents, your employees' emergency contact lists, and other essential records. ❖

Emergency Exit Map

(sample)



Telecommuting

Keeping Remote Employees Safe on the Job

MODERN TECHNOLOGY makes it easy for employees to work from home and remain connected to their employer. With telecommuting firmly entrenched among businesses today, companies that have allowed or are considering allowing remote work arrangements still need to make sure their employees have safe work environments.

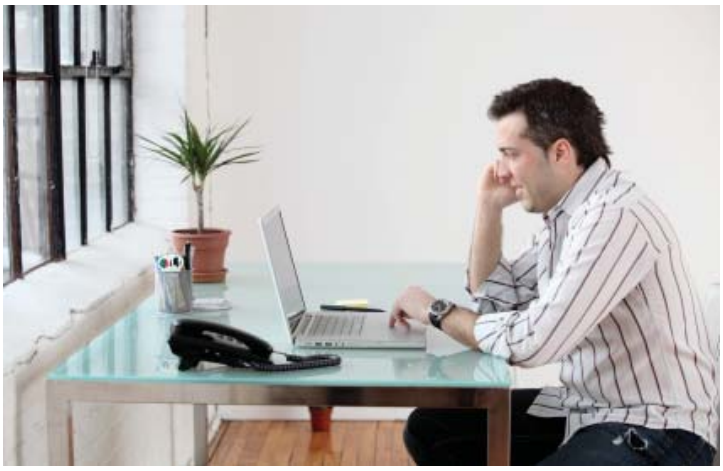
Fortunately, federal OSHA has addressed some of the safety issues surrounding remote employment. According to its guidelines, employers are required to maintain a safe workplace, even for employees working from their own home.

OSHA doesn't require an employer to inspect a remote employee's home work area. However, it may inspect the worksite of an employee performing an at-home job on behalf of their employer if it possibly involves health or safety hazards and there is a complaint. A record of all occupational illnesses and injuries must be kept on all at-home workers if an employer is subject to OSHA record-keeping requirements.

Keeping in mind that OSHA compliance measures should not involve controlling the home worksite of employees, employers may need to take some additional practical measures to ensure OSHA compliance.

As far as safety compliance goes, the absence of immediate supervision for remote workers is one of the main problems an employer faces. Employers should engage individual employees to actively participate in the safety process and take responsibility for their own safety. Whether at home, on the road or at a remote jobsite, remote employees need to be ready, willing and able to take the appropriate actions to protect themselves in any given situation.

Employee involvement in the safety process is crucial. Ask your remote employees to help you identify the work hazards and determine what is needed to prevent injuries to themselves and others during remote-location work. Most employers find that relying on the experience and first-hand knowledge of their remote staff is the best way to create safe remote worksites.



SAFE AT HOME: ***Laptop? Check. Sales call list? Check. Ergonomics? Maybe not! Engage off-site staff in company safety processes.***

Below is a checklist that you can employ to reduce safety hazards for remote workers. It is recommended for use by each telecommuter in organizing an alternate work site. The telecommuter should review the checklist with their supervisor prior to the start of telecommuting, and they are encouraged to work together to ensure the safety of the alternate work site. ❖

WORK SITE CHECKLIST

Work Area

___ The telecommuter has a clearly defined work space that is kept clean and orderly.
___ The work area is adequately illuminated with lighting directed toward the side or behind the line of vision, not in front or above it.
___ Exits are free of obstructions.
___ Supplies and equipment (both departmental and employee-owned) are in good condition.
___ The area is well ventilated and heated.
___ Storage is organized to minimize risks of fire and spontaneous combustion.
___ All extension cords have grounding conductors.
___ Exposed or frayed wiring and cords are repaired or replaced immediately upon detection.
___ Electrical enclosures (switches, outlets, receptacles, junction boxes) have tight-fitting covers or plates.
___ Surge protectors are used for computers, fax machines and printers.
___ Heavy items are securely placed on sturdy stands close to walls.
___ Computer components are kept out of direct sunlight and away from heaters.

Emergency preparedness

___ Emergency phone numbers (hospital, fire department, police department) should be posted at the alternate work site.
___ A first-aid kit should be easily accessible and replenished as needed.
___ Portable fire extinguishers should be easily accessible and serviced as needed.

Ergonomics

___ Desk, chair, computer and other equipment should be of appropriate design and arranged to eliminate strain on all parts of the body.