CORCORAN & HAVLIN INSURANCE GROUP

287 Linden Street
Wellesley, MA 02482
Phone: (781) 235-3100

77 North Street
Medfield, MA 02052
(508) 359-5555

Lougee Insurance
24 Bay Road
PO Box AC
Duxbury, MA 02331
(781) 934-6500

Inside This Issue:

The Corcoran & Havlin Insurance Group has been awarded the 2011 Reader's Choice Award for the 8th consecutive year.

RISK ADVISOR

Spring 2012

Corcoran & Havlin Insurance Group

- An insurance update for financial officers
- News, Views, & Current Events
- A publication of Corcoran & Havlin Insurance Group

MANAGING YOUR RISKS PROTECTING YOUR INTERESTS

Reducing Workers' Compensation Costs & the Experience Mod Factor

Has your workers' compensation premium recently increased? If so, it may be a result in your businesses' workers' compensation experience modification factor increasing. This article will examine how an experience mod is calculated and the impact it can have on your insurance costs.

An employer's workers compensation experience modification factor (mod) is the adjustment of manual premium based on previous loss experience. Experience mods are normally recalculated for an employer annually. Each year, a newer year's data is added to the three year window of experience used in the calculation, and the oldest year from the prior calculation drops off. The other two years worth of data in the rating window are also updated on an annual basis. Experience mods are usually calculated by NCCI (National Council on Compensation Insurance), but a few states have their own workers' compensation rating organization.

The experience modifier adjusts workers' compensation insurance premiums for a particular employer based on an evaluation of past losses of that employer in comparison to "average" losses of other employers in that state in the same business, adjusted for size. There are several things that a business owner can do to help lower their mod and insurance costs.

1. Be aware of the importance of getting injured employees back to work quickly. In many states employers receive a 70% discount for the injury on their experience mod if they return the employee to work before lost-wage payments begin. Additionally, employees who return to work, even in modified positions, save employers from lost-wage payments that increase the mod. Further, the longer employees are off the job, the less likely they are to ever return to work. It's a good idea for claim adjusters to work closely with physicians who specialize in workplace injuries, since they can more efficiently treat employees and may have more experience authorizing returns to work for light duty assignments.

2. Keep track of injured employees. There should be a process in place so employers report injuries to the insurer as soon as they occur. This allows the claim adjuster to better manage the process. An employer should work with the claims adjuster to make sure that he or she is making a maximum effort to get the injured employee back to work.

3. Correct job misclassifications. The experience mod reflects the difference between what the insurer expects to pay and what it actually pays for injuries. High-risk work causes the insurer to expect to pay more. If employers have employees that are misclassified on the workers compensation policy, their experience mod will be incorrect. Review the classifications with your Corcoran &

continued on page 4

C & H's Commercial Team

Patrick Byrnes

Mike Curtis

Bob Cleary

George Doherty

Debi Drury

Beth Eyster

Tom Fitzgerald

Tim Graham

Virginia Handerhan

Carolyn Jenkins

Jack Keefe

Mike Kennedy

Jane Loomis

Skip Lougee

Paul McDonald

Beth McDonough

Mary Mullin

Megan Peterson

Mark Sawyer

Susan Thomas

Kathy Uvanitte

Rick Weden

FIVE STAR SM
Award of Distinction

Protecting Your Company From Cybercrime

Protect your company from cybercrime. The most potent tools to fight this threat are to keep a wary eye and practice proactive online security techniques and policies. Below are several steps to protect personal privacy, banking information, and agency data, including adoption of recent advancements in banking security. What is Cybercrime? Like traditional crime, cybercrime covers a broad scope of criminal activity and can occur anytime and anyplace. What makes it different is that the crime is committed using a computer and the Internet. You may recognize some of its most common forms such as identity theft, computer viruses and phishing, and at a corporate level, computer hacking of customer databases. Most people are aware of these and protect themselves and their PCs with anti-spyware and anti-virus software such as Norton or McAfee programs. As a business owner, you should be alert to the fact that cybercrime is becoming more and more sophisticated and not only targets consumers and large corporations, but small to medium sized businesses as well. Single programs against these intrusions are not enough. An alarming cybercrime now affecting small to medium sized businesses is "corporate account take over." This involves cyber criminals penetrating the computer network of a business and spreading malicious software, such as a "keylogger" which records the words typed, Web browsing history, passwords and other private information. This in turn allows them access to programs using your log-in credentials. If they steal your password and breach your online banking system, the cyber criminal can begin an online session to initiate funds transfers, by ACH or wire transfer, to their accomplices. The accomplices withdraw the money almost immediately. Take the first steps to prevent fraud at your company – become aware of the latest cybercrimes and how they can access a business's computer network. A company should also employ the most up-to-date online security practices on a pro-active basis. Companies can also take the opportunity to present these online security practices to their clients, as many are also instituting internet-based online programs at their businesses.

Online Security Practices

While no tools or automated software is 100 effective, the best solutions to protect your agency are to be well informed and use common sense. Using a multiple vendor, multi-layer approach to system design can significantly reduce your chances of being a victim of cybercrime. To assess the risks associated with a cyber intrusion of your agency's online systems and critical client data, ask yourself the following questions:

1. Does your company have a hardware based firewall at the network level?
2. Does the network firewall include anti-virus, anti-spyware and anti-spam services along with content filtering and intrusion prevention, detection and real-time reporting?
3. At the individual PC level, does each computer have centrally updated and monitored anti-virus, anti-spyware and anti-spam software loaded?
4. Are your computers set up to automatically update your operating system and applications for the latest available security and critical updates?
5. Do you consider your browser security setting to determine how much or how little information the browser can accept from, or transmit to, a website?
6. Does your company have a security policy in place that includes such policies as disaster recovery, use storage of passwords, use of social media on work computers, etc.?
7. Does your agency back-up critical files in case of an issue that disables your systems?
8. Has your company identified an individual to review security policies and practices on an ongoing basis?
9. Are you aware of the laws governing the protection of personal information in your state?
10. Do you have cybercrime insurance to protect your data and liability exposure in the event of an intrusion?
11. Does your company have a training program to educate employees on best practices to avoid becoming a victim?
12. Does your online banking system provide multiple layers of security tools to prevent intrusions into the system such as token-based authentication?

continued on page 3

continued from page 2 ... Protecting Your Company from Cybercrime

Agency principals should consider the types of transactions they conduct within online banking and check with their banking institution for available security enhancements. These are just some of the basic steps an agency can implement to assess and protect itself from cybercrime. Your company should have a network security assessment and review conducted by a certified information technology firm that specializes in network security. This evaluation will help you to identify the "next steps" in securing your network and data from unauthorized access and distribution. If Your Company Becomes a Victim If you discover, or even suspect, your agency has fallen victim to corporate identity theft, you should proceed as follows:

- Immediately cease all online activity and contact your IT administrator.
- Remove the affected computer from the network and any other computer stations involved.
- Contact your financial institution to disable online access to the accounts and close affected accounts. You can then open new accounts and reset passwords.
- Consult your counsel and your state's data breach notification law and regulations to ascertain the process you need to follow.
- Notify other business partners that may have been affected, such as your insurance carriers.
- File a report with the police department. Common Online Fraud Definitions
- Malware refers to software programs designed to damage or do other unwanted actions on a computer system. Common examples of malware include spyware, keyloggers, and viruses.

- Spyware is a type of malware installed on your computer without your knowledge. It collects small to large pieces of personal information including Internet surfing habits. It can redirect web browser activity and change computer settings. Spyware is typically hidden from the user, and can be difficult to detect once installed without proper antispyware tools.
- Keyloggers, as with spyware, are installed on your computer without your knowledge. It is the action of tracking (or logging) the keys struck on a keyboard, typically in a hidden manner so that the person using the keyboard is unaware that their actions are being monitored. Keystroke logging can record the words typed, Web browsing history, passwords and other private information. This is extremely dangerous in all aspects of computer usage.
- Viruses are an ever changing and constant threat to all systems. Based on their digital makeup they can deliver malicious content to your data and systems in an effort to either collect data, destroy data, or turn your systems into a machine that spreads the virus or other malware.
- "Phishing" is the act of obtaining personal information or spreading malware using emails, calls, text messages or pop–up messages from what appear to be friends or legitimate banks, retailers, government agencies or other organizations. All of the security tips presented here are simply guidelines to aid companies in not becoming a target for cybercriminals. However, none can be guaranteed 100 effective.

C&H's Carolyn Jenkins Woman of the Year

Recently, at the annual meeting of the Massachusetts Association of Insurance Women (MAIW), at the Sheraton Colonial in Wakefield, MA, **Corcoran & Havlin's Carolyn A. Jenkins,** AAI, CIC, CPIW, DAE, LIA, CRIS, was presented the prestigious Member of the Year award for 2011–2012. The award was presented by Lora H. Lowe, CRM, CIC, CISR, CPIW, President of MAIW.

Carolyn has been active in the Norfolk Chapter of MAIW since 1982. On the local Chapter level, Carolyn had served in various positions – Director, Assistant Director, Secretary, Chairperson of Publicity, Public Relations and Audit Committee. On the State level, she had served as the State Chairman of Project InVest.

Corcoran & Havlin's Carolyn Jenkins and Lora Lowe, President MAIW

Did you know Corcoran & Havlin is on Facebook? Become our fan for up-to date news and articles relating to your insurance needs.

continued from page 1 ... Reducing Workers' Compensation Costs & the Experience Mod Factor

Havlin representative and make sure they are correct.

4. Review current open claims. The "unit start date" is when the insurer looks at the employer's business over the 3 year experience period (not including the most recent year) to determine what the insurer has spent and what it expects to pay on claims. So look at open claims before the unit start date and talk with your Corcoran & Havlin representative to ensure that claim data is adjusted properly and not incorrectly inflated.

5. Find out your company's minimum experience mod. In other words, where would the mod factor be if your company had not encountered any employee injuries during the period covered by the experience mod? Knowing this minimum mod means that you know how much of the insurance costs you can control. Some companies form safety committees to find more ways to reduce workplace injuries and to provide training that helps employees stay safe.

6. Canceling or rewriting a worker's compensation policy may negatively impact your experience mod. A cancel or rewrite of the workers' compensation policy will change how many months of experience will be considered on the experience mod. So if it is done at the wrong time, it can cause policies to stay on the experience mod longer than they would otherwise, driving up the experience mod.

For many companies, keeping down their experience modification factor is a vital concern beyond merely the cost of workers' compensation insurance. This is because increasingly, potential clients are using the experience mod as a rough benchmark of safety. Having a modifier above 1.00 can often shut out many kinds of businesses from bidding on important projects. The experience mod factor is an integral component of a company's workers compensation premium calculation, thus it is important that careful attention be paid to its accuracy and impact on annual insurance costs for your company.

CORCORAN & HAVLIN INSURANCE GROUP

www.chinsurance.com
Phone: (781) 235-3100
Fax: (781) 235-7190