HEFFERNAN INSURANCE BROKERS
Because You're Different

News You Can Use

Feb. 2013 Volume 1, Issue 4

WORKERS' COMP

How to Avoid Hiring Those Likely to File Claims

SINCE THE recession, hiring has become both easier and more difficult. On the one hand, the larger labor pool has made it easier to tap quality talent. At the same time, it's is far more difficult as many people looking for work have been off the job for an extended period of time.

Out of desperation, some applicants go to great lengths to present themselves in the best possible light, even though the facts may not support what's on their resume.

One danger is people who are serial workers' comp claimants, malingerers or have prior industrial injuries that can end up affecting your bottom line and X-Mod.

To avoid having one on your payroll, you may want to heed the following tips:

- **Dig deeper in references.** For smaller firms, vetting applicants is often limited to calling references they provide, and perhaps a drug test. Yet, even the basic step of contacting references can be made more effective by asking them if they know others acquainted with the applicant. By extending the reach, it's possible to obtain more information that can be helpful in evaluating prospective employees.
- **The integrity test.** This is one of the more effective tools for identifying job applicants who may be likely to file workers' comp claims. Employers often don't use integrity tests in the belief that they are too expensive. However, a study by Cornell hospitality professors Michael Sturman and David Sherwyn of 27,000 employees of a national hotel chain highlighted the value of using such a test.

Using one developed by American Tescor, the hotel hired 6,100 of 29,000 applicants. The researchers then used the data from the test and compared the workers' comp claims of the new hires to those of existing employees who did not take the test. The cost savings of screening workers was considerable.

Based on the number being tested, the cost of testing appears to be $8 to $14 per applicant. The study also found fewer workers' comp claims among new hires, which suggests that an integrity test can be a valuable tool for screening job applicants.

Because of the nature of the test, it can be administered before a job offer.

- **Avoid "medical baggage."** You should give applicants who have been given a job offer a pre-employment physical before being approved for hire. Many job applicants have been out of work for a long time during this economic downturn. When they are finally back to work, either in a position requiring physical labor or a sedentary one, which can lead to back and neck pain and repetitive injuries, they are often out of condition and can be prime candidates for workplace injuries.

You may be able to detect any "medical baggage" with a thorough physical exam.

See 'Tests' on page 4

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
San Francisco
Menlo Park
Portland
Chesterfield
Petaluma
Los Angeles
Santa Ana
New York

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

Cal License No. 0564249

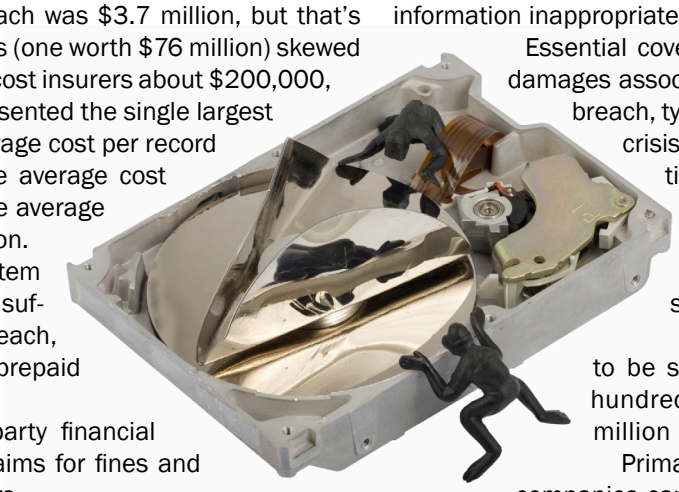
DATA BREACH STUDY

The Most Common Cyber Insurance Claims

WHILE THERE have been many articles on cyber breaches – especially major ones affecting big organisations – little has been written about the actual claims the affected parties are filing with their insurers. A recent report by cyber risk management services company NetDiligence is the most comprehensive yet on insurance-related aspects of cyber security.

The "Cyber Liability & Data Breach Insurance Claims" study found that personal identification information (PII) was the most exposed data type, followed by private health information.

The average claim per breach was $3.7 million, but that's only because a few large claims (one worth $76 million) skewed the average. The typical claim cost insurers about $200,000, and third-party damages represented the single largest component of claims. The average cost per record breached was $3.94, and the average cost of defense was $582,000. The average settlement cost was $2.1 million.



Third-party damages can stem from the direct financial loss suffered by victims of a data breach, such as stolen credit card or prepaid debit card information.

Besides liability for third-party financial losses, insurers are paying claims for fines and penalties imposed by regulators.

PII definition broadens

One interesting development, according to the report, is that the definition of PII has broadened, which doesn't bode well for businesses.

Writes NetDiligence: "In 2011, we saw a massive expansion in the types of information that regulators, litigators and the courts consider PII. After two monster breaches at large e-mail marketing firms (Epsilon and Silverpop), e-mail addresses are now arguably considered PII. Also, in February of 2011 the California Supreme Court found that zip codes qualify as PII for the purposes of California's Song-Beverly Credit Card Act. As a result of this holding, many class action suits have been filed against retailers in California, potentially costing them and their insurers many millions of dollars."

The extent of the financial pain can be significant. One company, insurer Health Net, has experienced two data breaches, one in 2009 and the other in 2011, the latter of which exposed the personal data of 2 million people.

The former incident involved the disappearance of a portable disk drive containing the personal data of 1.5 million people.

Health Net was fined by several states as a result of the breach, the largest fines being $375,000 in Arizona and $55,000 in Vermont.

Penalties for the 2011 breach could be significant, given that it was the second such incident involving the company.

Besides the threat of fines from states, companies whose records have been breached can also be hit with lawsuits. The last two years have seen a significant uptick in the number of suits alleging violations of customer privacy.

"It is clear that consumers and trial lawyers are testing the courts to determine whether a monetary value can (and will) be assessed when companies collect, share or retain customer information inappropriately," NetDilgence writes.

Essential coverage includes third-party liability for damages associated with a data or network security breach, typically bundled with related first-party crisis-management costs – forensics, notification, call-center staffing, credit monitoring and legal guidance.

The most common payout is for the costs of crisis management for smaller businesses.

That's because they are less likely to be sued in a class action on behalf of hundreds of thousands if not a more than a million "victims."

Primary coverage for small and mid-sized companies can expect to cost from around $5,000 to $15,000 per $1 million of coverage, and less for lower amounts of coverage, according to reports in insurance trade publications.

Larger outfits can expect to pay $15,000 to $35,000 per $1 million of coverage with low retentions. Bigger businesses and corporations are typically purchasing coverage with limits of between $5 million and $20 million.

Keeping the cost down

There are a few ways you can reduce your premium, including:

- Reinforcing your security practices before you apply – essentially, trying to qualify for a discount. This can be a twofold win, since it helps to decrease the cost of coverage as well as your overall risk to a breach.
- Implementing strong password protection. Most cases of hacking can be traced to weak passwords that were either not encrypted or not changed regularly. If you have multiple passwords for multiple services, you can purchase a password management solution.
- Conducting regular risk assessments to reveal hardware, software and individual site vulnerabilities.
- Creating a written IT security policy that identifies critical assets and defines policies for physical security, account management, and backup and recovery, among other areas.
- Leveraging firewalls, virtual private networks, anti-virus and anti-spam software and secure mobile solutions in order to secure network access and mobile devices. ❖

HUMAN RESOURCES

Tips for a Viable Workplace Social Media Policy

AS SOCIAL media use permeates almost every level of society, employers have found there is little they can do about their employees visiting sites such as Facebook and Twitter while on the clock.

No matter how stringent the rules you lay down, the temptation is too great for your staff to steer clear of these sites while they work.

A new report by the law firm Proskauer Rose LLP, "Social Media in the Workplace around the World 2.0," sheds light on notable developments in the use of social media in the workplace, and what employers do to regulate it..

With this report in hand, it makes it easier for you, as an employer, to lay down workable social media rules that should not infringe on your employees' perceived right to engage in the practice, but at the same time protect the best interests of your company, while safeguarding your company secrets.

The Proskauer report identified five universal best practices for controlling social media use in the workplace. They are:

- **Implement a policy dedicated to social media.** Implement a policy that clearly sets out acceptable and unacceptable usage inside and outside the workplace, as well as after employment with your company ends. Make sure that your company policy complies with any applicable state laws, including privacy legislation.

While it is legal to completely bar employees from using social media during work – either on company-supplied devices or their own – there is one exception. You must avoid infringing the rights of your staff to engage in protected concerted activities under section 7 of the National Labor Relations Act (NLRA) – see below.

- **If you do monitor, abide by the law.** If you want to monitor you employees' use of social media in the workplace, you need to make sure that your policy explicitly states the extent and nature of this monitoring. Employers must also comply with and implement their policies in accordance with local requirements.

If you do collect personal data as a result of any monitoring, you should store it safely, and make sure it is not tampered with, disseminated further or stored for any longer than necessary. Make sure your policies allow you to document any misuse of social media sites by employees.

Also, keep in mind that any monitoring of social network use (and related policies) must account for the rights of workers to engage in certain collective activities, known as protected concerted activities (such as organizing co-workers, complaints about working conditions, on-the-job protests, picketing and strikes) under section 7 of the NLRA, and the prohibition against employers interfering with or restraining employees against exercising such rights (under section 8 of the NLRA). In particular, employers must not engage in monitoring that has the effect of explicitly or implicitly restricting employees' rights to engage in such activities.

- **Use a monitoring system that's appropriate.** Any monitoring should go no further than necessary to protect the employer's business interests. You should assign an employee who has been trained to understand the permissible types of monitoring and the need to comply with state privacy laws. This includes issues relating to safe storage, confidentiality and onward transfer of personal data.

The key here is balancing the necessity to protect your company's interests against your employees' privacy rights.

- **Use information from social media with care when hiring or disciplining employees.** If you are going to rely on such information, please keep in mind that it could be inaccurate. Not only that, but you could be setting yourself up for claims of discrimination, breaches of data privacy and privacy infringement.

Recently, a number of states have enacted laws barring employers from requiring that job applicants supply them with their social media passwords, but even the act of using information from their social media pages could land you in hot water if you use what you learn incorrectly or illegally.

And, if you are mulling disciplinary measures based on information from social media pages, you must balance their employees' rights to free speech and privacy with business considerations.

- **Protect your firm's confidential information.** You should address concerns about divulging company information through social media policies. And you should also include the explicit coverage of social media in provisions dealing with misuse of confidential information. ❖

WORKERS' COMP

Surprised Your X-Mod Changed? Here's Why

IF YOU are an experience-rated employer and your policy renewed on Jan. 1, you may have noticed changes to your X-Mod that may or may not have been welcome news.

Changes made to the California Workers' Compensation Experience Rating Plan that took effect Jan. 1 were aimed at making X-Mods more accurately reflect employers' claims histories.

But the changes resulted in some employers seeing major swings in their X-Mods, increasing them up to 15%, sometimes even more.

The result for some employers was a double-whammy price hike from not only increasing rates filed by insurers, but also premium increases based on higher X-Mods.

While the majority of employers (64%) saw swings in their X-Mods of plus or minus 3 points,

- 17% saw decreases of 4-10 points,
- 4.7% saw decreases of 11 to 15 points,
- Less than 1% saw decreases of more than 15 points,
- 9% saw increases of 4-10 points,
- 2% saw jumps of 11-15 points, and
- 3.4% saw increases of more than 15 points.

The Rating Bureau calculates experience rating modifications by comparing an employer's actual claim costs to the average claims costs expected of all employers of similar size and industry classification. The formula takes into account how much credibility to assign to the experience of an individual employer.

For large employers, actual claims experience is considered a good indicator of future claims experience. In other words, larger employers have higher credibility values.

But small employers' claims experience can be volatile and more a function of chance. As a result, small employers are assigned lower credibility values in the experience rating formula.

That's changed under the new Experience Rating Plan. On Jan. 1, the Bureau started assigning more credibility to most employers' actual claim history. And in light of the Bureau's prior practice, smaller firms are likely to see the biggest swings in their X-Mods as a result of the change.

"In other words, for most employers, all else being equal, somewhat greater weight is being given to their own claim experience," the Rating Bureau said. "Employers that have better than average experience will generally receive a lower credit experience modification in 2013 than they would have received in 2012. Conversely, employers that have poor experience will generally receive a higher experience modification."

The Rating Bureau has regularly been updating the Experience Rating Plan ever since the insurance commissioner's 2008 Experience Rating Task Force recommended that it do so.

"As the payroll and claims experience of California experience-rated employers evolves, so too must the credibility values in order to maintain the Experience Rating Plan's actuarial balance," the Rating Bureau wrote.

The last change to credibility values was in 2010. ❖

Continued from page 1

Drug Tests Can Reveal More Than Just Illegal Use

- **Background checks.** You should consider a comprehensive check by a private investigation firm, particularly for staff who will be driving their own or company vehicles. If they have a record of traffic violations or DUIs, this can spell trouble. A background check can also reveal if a candidate has misrepresented their workers' compensation history or medical condition. This can uncover a history of false claims or demonstrate that the applicant is a safety risk based on medical opinion.
- **Drug testing.** This is not just a matter of identifying illegal drug use, as a test may indicate an applicant is taking one or more prescriptions for a previous job-related injury. Remember, you need to comply with state and federal laws when drug testing.

The Take-away: The goal is to obtain as much accurate information as possible regarding an applicant so the picture is complete and reliable.

While it takes time and costs more, the expense pales to the cost of hiring someone with a propensity for filing a workers' comp claim or suffering a workplace injury. ❖