CYBER RISKS & LIABILITIES_
NEWSLETTER

May/June 2015

IN THIS ISSUE

Tailoring a Cyber Policy to Your Business

Cyber insurance coverage is a relative newcomer to the insurance market, which can present some challenges for both businesses and insurers. To date, there are no official industry standards for cyber insurance, but there have been major strides in recent years to establish some. The National Institute of Standards and Technology (NIST) offers a comprehensive overview of the current state of cyber risk management. Adherence to these standards is currently voluntary, but many experts believe that the NIST recommendations have become the unofficial industry standard for cyber risk management.

Still, with the breakneck pace of technological evolution and increasing pressures to digitize data, most businesses are already vulnerable. The best way to protect yourself and your business is to conduct a risk assessment and identify any gaps in your coverage. Here are a few things worth looking for:

Understand the coverage that you have, and the coverage that you don't. Many people might make the mistake of assuming that a commercial general liability (CGL) policy covers losses in the event of a cyber attack. However, assumptions like that can be dangerous and costly, as many CGL policies specifically exclude electronic data. Take the time to review your current coverage and identify any exclusions that might leave you vulnerable.

Understand your company's specific needs. Companies vary in their use of and dependence on data. For instance, customer data held by financial or health care businesses is comparatively more valuable to criminals. Other companies, like online merchants, may potentially suffer greater losses as the result of an attack that crashes a website or interrupts service. Different policies have different limits, sublimits and exclusions for different kinds of losses, so it's important to work with an expert who can find exactly where your liabilities lie and what kinds of coverage you need.

Consider retroactive coverage. Unfortunately, cyber breaches often go undetected for a long time. As a result, a policy that only offers coverage to the date of inception might leave you vulnerable to a cyber attack that hasn't yet been discovered. To mitigate your liability as much as possible, get coverage with the earliest possible retroactive date.

Obtain coverage for third-party vendors. Many businesses outsource their data processing or storage to a third-party vendor. This is a smart move, especially if you aren't equipped to handle the IT side of your business. Unfortunately, it may leave you liable for damages if the actions of that third party are responsible for a breach. Make sure you have coverage for the actions or omissions of third parties with whom you do business.

The best way to determine your specific risks and liabilities is to talk to an expert. Consult with your broker at The Robbins Group to identify your risks and tailor a cyber policy to fit your specific needs.

The Robbins Group & Regency Employee Benefits
Divisions of ACRISURE

Lessons Forgotten: Harrowing Reminders from Verizon's 2015 Data Breach Investigations Report

When Verizon released its annual report on data breaches, the biggest shock might have been how little had changed from last year's report. Businesses ignored known vulnerabilities and failed to implement simple fixes, resulting in losses that could have easily been prevented. The report identified a number of key areas that have been breached, but some stood out more than others. Here are three of the most frightening takeaways from the report, and what you can do to protect yourself:

- **Old vulnerabilities**: 99.9 percent of vulnerability exploits occurred more than a year after the vulnerability had been identified. Worse, almost 97 percent of exploited vulnerabilities came from a list of just 10 disclosed vulnerabilities. A few patches would have eliminated almost all of these incidents. It's a simple fix, and one that your business can't afford to ignore.

- **Phishing still matters**: Phishing relies upon the law of large numbers, and with a large enough audience, success is almost guaranteed. According to the report, "a [phishing] campaign of 10 emails yields a greater than 90% chance that at least one person will become the criminal's prey." Malware filtering has improved, but it isn't perfect. Employee awareness is the last, and best, line of defense against malware in email.

- **Privilege abuse**: According to the report, 55 percent of insider incidents involved the abuse of privileges. Auditing and fraud-detection can only do so much, and often after the damage has already been done. Consider reducing and controlling privileges instead. It might make certain tasks slightly more inconvenient, but protecting sensitive patient or client data is worth it.

Small Businesses Most Vulnerable to Cyber Attacks

According to the 2015 Small Business & Cybersecurity survey, 81 percent of small business owners think that cyber security is a concern for their small businesses, while 94 percent either frequently or occasionally think about cyber security issues.

Surprisingly, only 42 percent of respondents had invested in cyber security protection in the past year, despite the fact that 31 percent of these businesses had experienced either a successful or attempted cyber attack.

It's possible that small business owners might simply be spreading themselves too thin. About 83 percent of small business owners said that they handle cyber security themselves. But given the threat, it was surprising to discover that 95 percent of small business owners don't have cyber insurance.

Protecting Yourself from Ransomware

Cyber security experts at the FBI recently warned that ransomware attacks may be on the rise. This type of malware actually encrypts your data, then demands that you pay a fee in order to access it. With ransom sums often amounting to thousands of dollars, consider taking these simple steps to protect yourself from ransomware:

- Use trustworthy anti-virus software and make sure it is up to date.
- Enable automated updates of your operating system and browser.
- Only download software from trusted sites.
- Never open attachments in unsolicited emails, even if they come from people in your contacts.
- Never click on a link in an unsolicited email.
- Make sure to back up your data regularly and store it offline.

Preventative measures are important, but they can't account for everything. Consult with your broker at The Robbins Group to go over your policy and look for any gaps in your coverage.

CYBERRISKS&LIABILITIES_
NEWSLETTER

The Robbins Group
330 Superior Mall
Port Huron, MI 48060-3833
(810) 987-3500
http://www.robbinsgroup.com