Cyber Risks & Liabilities

Second Quarter 2019

5 Ways to Reduce Your Data Exposures

Cyber security threats and trends can change year over year as technology continues to advance at alarming speeds. As such, it's critical for organizations to reassess their data protection practices regularly and make achievable cyber security resolutions to help protect themselves from costly breaches:

1. **Provide security training**—Even the most robust and expensive data protection solutions can be compromised should an employee click a malicious link or download fraudulent software. As such, it's critical for organizations to thoroughly train personnel on common cyber threats and how to respond. Your employees should also know your cyber security policies and know how to report suspicious activity.
2. **Install strong anti-virus software and keep it updated**—Outside of training your employees on the dangers of poor cyber security practices, strong anti-virus software is one of the best ways to protect your data. Organizations should conduct thorough research to choose software that's best for their needs. Once installed, anti-virus programs should be kept up to date.
3. **Instill safe web-browsing practices**—Deceptive and malicious websites can easily infect your network, often leading to more serious cyber attacks. To protect your organization, employees should be trained on proper web usage and instructed to only interact with secured websites. For further protection, companies should consider blocking known threats and potentially malicious webpages outright.
4. **Create strong password policies**—Ongoing password management can help prevent attackers from compromising your organization's password-protected information. You'll want to create a password policy that requires employees to change their password on a regular basis, avoid using the same password for multiple accounts and use special characters. Long passphrases are becoming increasingly popular as well, and may be a good option for your organization.
5. **Get vulnerability assessments**—The best way to evaluate your company's data exposures is through a vulnerability assessment. Using a system of simulated attacks and stress tests, vulnerability assessments can help uncover entry points into your system. Following these tests, security experts can compile their findings and provide recommendations for improving network and data safety.

WATKINS INSURANCE GROUP

Watkins Insurance Group
3834 Spicewood Springs Road, Suite 100
www.watkinsinsurancegroup.com

Cyber Criminals: Who Are They and What Motivates Them?

While we commonly think of cyber criminals as singular individuals bunkered up in a basement, the truth is that attackers are often much more sophisticated. Let's examine the most common threats to your business:

- **Insiders—**While your employees are some of your best assets, they can also be one of your greatest threats. In some cases, well-meaning employees accidently put confidential information at risk through careless cyber security practices. Other times, disgruntled employees will vandalize assets or steal proprietary data to get back at your organization.
- **Organized crime—**Organized cyber criminals are primarily interested in money. These groups often seek personally identifiable information like social security numbers, health records, credit card details and baking information. They then hold this information hostage through ransomware or sell it outright on the dark web to turn a profit.
- **Hacktivists—**Hacktivists operate with a political agenda, often carrying out high-profile attacks to distribute propaganda or damage organizations they disagree with. Hacktivists typically fall under the category of cyber vandalism and look to damage reputations or steal incriminating information.
- **Government-sponsored groups—**These cyber criminals are well-funded and are typically motivated by political, economic, technical or military agendas. Government-sponsored attacks are often very sophisticated, and these groups target highly sensitive and competitive proprietary data. These types of attacks often use multiple hacking strategies occur over a long period of time.

Cyber Insurance Policy Considerations

One of the best ways for businesses to protect themselves against cyber exposures is with proper insurance. However, cyber liability insurance policies do not offer one-size-fits-all protection, and businesses need to keep some considerations in mind if they are to secure the right coverage. The following checklist provides a road map to reviewing cyber insurance policies:

- Does your policy cover the cost of retaining a forensic investigator to review data breaches? Does your policy limit your selection to a single investigator?
- Does your policy have a sublimit for forensic investigation-related costs? Is your sublimit in line with the average cost of retaining a forensic consultant?
- Does your policy cover the cost of printing and mailing notification letters?
- Does your policy cover the cost of staffing call centers to handle consumer questions regarding a data breach?
- Does your policy exclude coverage for notifications that are not expressly required by law?
- Does your policy have a sublimit for the total costs of issuing consumer notifications? Is this sublimit in line with the number of consumers your organization serves?
- Does your policy cover the costs of providing credit monitoring, identity restoration and identity theft insurance services?
- Does your policy require your organization to use a certain company for credit monitoring-related services? Does this third party have a good track record?
- Does your policy have a sublimit for the total cost of credit monitoring? Is the sublimit adequate enough to cover the average cost of credit monitoring multiplied by the number of consumers you serve?
- Does your policy cover any regulatory proceedings that may occur as the result of a breach? Does your policy cover legal fees, fines or penalties that may incur as a result of a breach?
- Are sublimits in line with the average cost of defending a regulatory investigation for your industry?
- Does your policy include protections for contractual liabilities that result from a data security breach?
- Does your policy cover contractual liabilities that may be owed to a payment processor or merchant bank?

Cyber insurance can be complex, and it's critical to work with a qualified insurance broker. To learn more about your options, contact Watkins Insurance Group today.