Firms Bolstering Investment in Cyber Insurance to Transfer Risk

As cyber breaches rise, communication planning evolves.

By Ioana Good

Mitigating risks is a hot topic these days. Law firms store a great deal of sensitive information that has value to hackers who can gain access to it and profit from it. Arguably, there is no greater risk to a firm than a crippling cyberattack that can have long-lasting impacts on business operations and damage its reputation. One of the most common ways for firms to mitigate cybersecurity risks is through cyber insurance. Like other forms of insurance, this is a mitigation strategy that involves risk transference – when a third party assumes a great deal of the risk for an agreed-upon fee.

While cyber insurance will not prevent a successful cyberattack, it does provide a mechanism for firms to recover the costs of responding to such an attack. Cyber insurance is a contract between a firm and an insurer to protect against losses that relate to network or computer incidents. Firms recognize an increased responsibility for their cybersecurity, and to price policies, insurers want to know a fair amount about how each company protects itself.

Additionally, as users demand more digital tools for remote work, collaboration, and learning, communication planning will also play a critical role and need to be integrated. Upper management and communication professionals will communicate quickly during a cyber attack and have management processes, communication plans, metrics, and reporting in place. "Unfortunately, this is the world we live in, and firms will experience an increased pressure to gather all the information, uncover the root of the issue and respond in a meaningful way without elevating the crisis," says Heather Oden, COO at Ball Janik LLP. "We must be proactive as cyberattacks continue to cause widespread disruptions in business."

If you are a business connected to the internet and you store and send electronic information, cyber insurance may be for you. Yes, just about all of us fit that category unless you're doing some secret squirrel stuff in a bunker for the NSA. But kidding aside, it is essential to examine if the type of data you store is likely valuable to hackers. For instance, if you work with intellectual property, you have data that is likely a high-risk target for attackers. If most of your work involves otherwise publicly available data, you're a lower risk target. However, there is still the potential for a ransomware attack on both high and low-risk targets that can cripple your business. Ransomware involves a hacker gaining access to your data and then encrypting the information so that it can only be accessed by someone who has the decryption key. Basically, your data is held for ransom. A cyber insurance policy may provide a great deal of help if you become a victim of this type of attack.

How much you will pay for cyber insurance depends on several factors. Certainly, the size of your business and the annual revenue will be considered. The type of data that you deal with will impact the cost. If you are an organization that has a history of cyber attacks and your security is poorly rated by the carrier, you will pay more. Finally, the industry you are in plays a factor in the cost of insurance. Healthcare and financial companies will find a higher price tag to transfer cyber risk to insurers.

"Cyber breaches continue to happen at an alarming rate, and we must be prepared," says Oden. "While we can't expect cyber insurance to fix all our issues, it does help provide an offset of the costs to respond if you are a victim of an attack; this is another tool to help us protect our firms."

Ioana Good is a regular contributor to The Mid-Market Report and the New York Law Journal. She is the founder of Promova, an international communication, PR, and branding agency. For any questions, reach out to igood@getpromova.com.