Cyber Insurance – Some Questions to Ask

Description

Reports of large-scale data breaches, hacking and cyber attacks appear in the media almost daily. The recent Equifax breach alone has exposed sensitive personal information of over 143 million Americans. Phishing and ransomware attacks are also on the rise. Phishing attacks are used to steal user data, such as bank account or social security numbers or log-in credentials. In a ransomware attack, the attacker encrypts a company's data and makes it unavailable to the company until a "ransom" of some amount is paid.

One common misconception is that these cyber attacks only happen to large companies. In reality, attackers also frequently target medium and small businesses, but you are less likely to hear about them on the news. A recent study by the security firm Symantek reports that 31 percent of all breaches occur at businesses with 100 or fewer employees. Small businesses are particularly at risk because they typically do not have access to the same level of resources as a large business to protect themselves.

Cyber attacks can cause harm to a business in a number of different ways. A company will incur costs to investigate the cause of the attack and to recover data and systems, not to mention the potential ransom fee to "unlock" a company's data. In addition, after a cyber attack occurs, the target business also may incur costs to investigate the breach, to notify customers and other third parties (such as regulators and attorneys general) if sensitive information is involved, and to defend and settle lawsuits involving claims that the company did not act properly in protecting the data.

One recent survey estimates the average cost to a United States business for each lost or stolen record containing sensitive information is $225, and the average total cost of a data breach or cyber attack to be about $7.35 million. Few businesses can absorb such costs without crippling, adverse effects.

Many companies are surprised to discover that their general commercial liability policies do not cover most types of cyber risks. Commercial general liability policies typically only cover bodily injury and property damage, not monetary losses, ransom costs, or regulatory fees and expenses. In addition, coverage is often limited to losses caused by "tangible" means. Insurance companies typically consider data breaches to be "intangible" causes not covered by the policy. Most commercial general liability policies also include an exclusion for access to or disclosure of confidential information, and the resulting liability.

Cyber insurance is still an emerging product. There are differences in services and coverages, as well as in the services for which the policy will pay. When reviewing policies for clients, insurance advisers should take the time to understand the client's business, as well as to understand the coverages and services provided by each carrier under its policies.

Here are some questions to ask when you are investigating cyber insurance policies for clients:

- What data does the client have, and where is the client at risk for a cyber attack? Most businesses have some data, such as credit card data or employee information, that can be compromised.
- Does this policy have first party and third party coverage? If so, what risks are covered and what risks are not covered? Are these risks for which the client's business needs coverage?
- Does the client need a computer fraud endorsement to a fidelity bond or crime prevention policy? Some cyber liability policies only cover losses caused by unauthorized access to a company's system by a third party, and do not cover the situation where a transfer is made by a business's employee after receiving fraudulent instructions to do so. Endorsements to the client's other policies may be needed to cover the gap.
- What are the policy limits and sublimits? All policies will have limits on coverage and many will have

sublimits on certain payments (for example, the costs of forensic investigations). Are the sublimits reasonable in light of the likely average cost to the business if a cyber attack occurs?
- What are the policy retention and subretention amounts? If the retention amount is very high, the insurance may not be of much benefit to the business except in extreme cases.
- Does the policy contain clauses that limit the insured's ability to use self-help to mitigate damages following a breach or potential breach, or subrogation clauses that allow the insurance company to seek reimbursement from the insured's clients or customers or vendors for claims paid under a policy that might have been caused by such parties? Can these clauses be removed or modified?

Defending against cyber attacks has become a cost of doing business for all businesses, not just large companies. The first defense is to have consistent policies and procedures in place that are followed by all employees and others who have access to confidential data. As a backstop, cyber insurance can be an important part of that defense for many businesses. However, businesses need to understand that not all cyber insurance policies are created equal, and need proper advice to understand and properly protect against their risks.

John E. Ottaviani (jottaviani@psh.com), Colin A. Coleman, and David J. Pellegrino are partners at Partridge Snow & Hahn LLP, a New England business and litigation law firm based in Providence, Rhode Island.

Date Created
January 15, 2018