Is Your Business Insured Against A Cyber Attack?

(October is National Cybersecurity Awareness Month. This is another in a series of PS&H articles related to cyber risks and security).

Your business has insurance coverage for flood and fire damage. You are protected if an employee gets into a car accident. But are you covered for a cyber attack?

Cyber attacks can be expensive. One recent survey estimates the average cost to a United States business for each lost and 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.

Cyber attacks can cause harm to a business in a number of different ways. Employees and employers can access data or distribute sensitive company information or trade secrets. Malware or ransomware can be introduced to your company's computer system and damage or destroy your company's data, or can "lock-up" your company's data until a ransom is paid. So-called "phishing" attacks can permit a third party to obtain money or information from your company's accounts, either directly or through unsuspecting employees who act on false information contained in fraudulent emails. In addition, after a cyber attack occurs, your business inevitably will 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 your company did not act properly in protecting the data.

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 or regulatory fees and expenses. In addition, coverage is typically limited to losses caused by "tangible" means. Insurance companies typically consider data breaches to be "intangible" causes not covered by the policy.

Some insurance companies offer a cyber liability endorsement to the commercial general liability policy for relatively little expense. But these endorsements can provide a business a false sense of security. Many of these endorsements only have what is called "first party coverage." These policies only cover a company's own losses, such as the cost resulting from a loss of the company's own data, the cost of forensic investigations to determine the source of a breach, the cost to recover lost data, costs paid to someone as a "ransom" to get your data back, or legally required notification costs due to a cyber incident. Thefts of customer information, claims by customers and other third parties that your company failed to properly protect the third parties' sensitive information, and litigation defense and settlement costs may not be covered unless you also have "third party coverage," and even then, the coverage may be limited. Whether your business obtains an endorsement to a general commercial liability policy, or a stand-alone cyber liability policy, you need to evaluate whether the policy provides both first and third party coverage.

Here are some questions to ask your advisor when you are looking at cyber insurance policies:

- 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 our business needs coverage?
- Do we need a computer fraud endorsement to a fidelity bond or crime prevention policy? Some 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.
- 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? Similarly, most policies have retention amounts, also known as “deductibles”, which the insured business must pay before the insurance company starts to pay under the policy. 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?
- If your company is regulated, does the policy contain coverage for regulatory risk?

Defending against cyber attacks has become a cost of doing business for all businesses, not just large companies. Cyber insurance can be an important part of that defense for many businesses. However, businesses need to understand the language of cyber insurance policies to make sure that coverage is adequate, and should consider engaging an independent attorney or advisor to review such policies for sufficiency in light of the company’s business.

Date Created
October 19, 2017