Bringing Your Business Online: Cyber Insurance

Description

By John Ottaviani

The current COVID-19 pandemic has forced many businesses online in order to survive. In many cases, businesses had no plans to be online. Others were forced to move online more quickly than planned. In order to assist these businesses, we have prepared a series of articles discussing some of the more important legal issues to address when moving your business online. Website Terms discusses online terms and conditions to protect your business. Privacy Policy discusses how your business collects, uses and discloses personal information of others. Third Party Content discusses the risks of copying photos, music, videos, and other content created by third parties onto your website. E-Commerce Policies discusses e-commerce policies that a website selling products or services should have in place. Creating Enforceable Contracts discusses the safest method to ensure that you can enforce your online terms and conditions protecting your business. Written Information Security Programs (WISPs) discusses several reasons why it is important for all businesses to prepare a WISP and to keep it updated. Protecting Your Brand discusses the process of selecting and protecting your brand.

Cyber Insurance

Bringing your business online introduces new risks, including the need to have more digital data about your customers, such as credit card information, names, addresses, contact information, and purchase history. Some of that data may be stored on your company's computers, and some may be stored with a third party vendor in the "cloud."

All of this digital data is vulnerable to attacks by third parties who want to access it. Cyber attacks can cause harm to your business in a number of different ways. You will incur costs to investigate the cause of the attack and to recover data and systems, and may be forced to pay a ransom fee to "unlock" your company's data. In addition, after a cyber attack occurs, your 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 your company did not act properly in protecting the data.

A common misconception is that these cyber attacks only happen to large companies. In reality, attackers frequently target medium and small businesses, but you are less likely to hear about them on the news. A recent study reports that over 40 percent of all attacks 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.

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.

One important tool to reduce the risk is a cyber insurance policy. There are many differences among policies, so it is important to discuss coverage with an insurance broker or agent with experience in this area.

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

- **What data does your business have, and where are you at risk for a cyber attack?** Most businesses have some data, such as credit card data or employee information, that can be compromised.
- **Does your policy have first party and third party coverage?** First party coverage pays for damages resulting from a breach of your company's computer system. Third party coverage pays for damages resulting from a breach of data you have given to a third party vendor. It is important that most businesses have both types of coverage.
- **What risks are covered and what risks are not covered?** Are these risks for which your business needs coverage?
- **What are the policy limits?** 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 your business if a cyber attack occurs?
- **What are the policy retention (deductibles) amounts?** If the retention amount is very high, the insurance may not be of much benefit to your business except in extreme cases.

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.

If your company would like assistance with cyber insurance, we would be happy to discuss your requirements and assist you. Partridge Snow & Hahn Partner John Ottaviani has over 25 years of experience bringing businesses online and can provide the guidance needed to make the transition as painless as possible. He can be reached at jottaviani@psh.com or 401-861-8253.

To download a PDF with the entire Building Your Business Online series of articles, please complete the form below.

Date Created
July 16, 2020