Risk Management Blind Spot

Understanding your Company's Cyber & Network Privacy Liability

Cyber Security - It's the risk management "blind spot" that is quickly becoming a more obvious concern to many business owners. In this month's newsletter, we want to highlight the topic of network security. We invite you to put on your "risk manager" hat for a couple of minutes as we touch on a risk area that you may want to ponder in relation to your company's insurance and risk management programs.

If it is not already on your radar, you may be wondering what the exposure even looks like. There are several areas of Cyber Risk, but we will broadly categorize them into First Party Losses and Liability Losses.

"Security is, I would say, our top priority because for all the exciting things you will be able to do with computers... organizing your lives, staying in touch with people, being creative; if we don't solve these security problems, then people will hold back. Businesses will be afraid to put their critical information on it because it will be exposed." - Bill Gates

First Party Risk

Compromised Personally Identifiable Information (PII): Privacy breach is the risk that is most often thought of when a business is concerned with Cyber Security and their risk exposure. The average cost of a data breach has been estimated at over $200 per lost record, including the cost of lost customers, PR expenses, and notification costs. When a company finds itself in a situation where PII has been compromised, there is a need for a quick response, forensics, and proper notifications to the affected individuals. Most states, including Michigan, have enacted privacy laws which require notifications be made in the event of data breaches. Failure to provide proper notices can result in fines, according to Michigan's Identity Theft Protection Act. Privacy breaches and loss of digital assets can stem from a variety of causes, such as theft, human error, hacking, improper disposal of data, etc.

***Virus*:** When a malicious code is launched, the outcome can be disastrous. Denial of service attacks can cause substantial business interruption losses, not to mention the costs to shore up the security of the system and repair the damage.

***Cyber Extortion*:** Believe it or not, there are losses due to extortion. An example would be a hacker gaining access to data, then demanding payment in return for not making the data public.

Liability Risk

Lawsuits: In short, there is the risk of a third party taking action against your company. A private party may take action by means of a lawsuit. An Attorney General may take regulatory action against a company for a major data breach. In either of these scenarios, defense costs can mount quickly, creating financial stress long before a verdict is reached, the case is settled, or any fines are levied.

Solutions

We offer these examples to help you consider the possible exposures your business may face. Standard insurance policies are typically not constructed to cover this exposure. However, there are several insurers who have crafted Cyber Liability insurance products in response to the growing Cyber and Network Privacy risk. Available coverage ranges from add-on endorsements which provide a modest level of coverage, to stand-alone policies which include loss control and claims services specifically geared towards Cyber losses. If you are unsure what your current insurance program covers, we are available to discuss your risk with you, review your current policies, and prepare a gap analysis.

Not every business has a Cyber Liability exposure that is large enough to insure; however, if you feel that yours does and you would like to talk to one of our Business Insurance Advisors to learn more, please contact us.