Cullen | Dykman

The Growing Need for Cyber Insurance in the Post-COVID-19 World

June 17, 2020

Cybersecurity has emerged as a growing concern for businesses given the increasing risk of falling victim to a data breach or other cyberattack in recent years. The COVID-19 pandemic has created additional cybersecurity issues as most employees are now working from home and using a variety of digital platforms and programs. While many businesses may already have some form of cyber insurance, the enhanced cybersecurity risks created by more employees working remotely has only further accentuated the need for nearly all businesses to invest in cyber insurance. Moreover, businesses that already have cyber insurance should review their policies to determine what their policy covers, including whether their cyber insurance policy will cover data breaches or cyberattacks that occur while employees are working from home.

What is Cyber Insurance?

Although data breaches and cyberattacks are not new, cyber insurance is still in its infancy. The coverage provided by the vast majority of general business liability policies are limited to incidents involving bodily injury or damage to property. In recent years, some insurance companies have created and issued cyber insurance policies separate from general business liability policies that specifically protect businesses in the event they suffer a data breach or other cyberattack.

Cyber insurance can help businesses cover the cost of a cyberattack, including coverage of legal fees incurred as a result of the attack and other expenses. These other expenses include costs associated with notifying affected parties or customers that personal information may have been compromised due to a data breach or cyberattack, repairing damaged systems following an attack, and recovering data that may have been lost.

Many business owners and executives are unaware of how expensive dealing with a cyberattack can be until it is too late. For example, in 2013, Target retail stores suffered a massive data breach that resulted in the credit card information of approximately 40 million customers to be compromised. Target estimated that the data breach cost the company between $200 and $300 million after settling various lawsuits related to the breach. While reports indicate that Target was able to recover some of these funds through insurance, it is estimated that their out-of-pocket loss from the breach was over $100 million.

Cyber Insurance and COVID-19

The COVID-19 outbreak has significantly increased the risk of businesses falling victim to a cyberattack as hackers seek to take advantage of many employees being quickly forced into new working environments. Because of this, it is more important than ever for businesses that do not have cyber insurance to consider obtaining some form of cyber insurance coverage or to review existing policies to ensure coverage for an attack that may occur due to remote work.

Some policyholders may be surprised to learn that their cyber insurance policy contains language that can be construed as excluding coverage from cyberattacks that occur while employees are working from home. Specifically, the definitions of certain terms in cyber insurance policies may be written in such a way to only include hardware or networks that are within the insured business's direct control and thus exclude attacks that occur while employees are working with their own computer and using their own internet connection. For example, the term "Computer System" in a cyber insurance policy may be drafted to only include "hardware owned by the insured and operated on behalf of the insured's business." Policyholders and those seeking to purchase cyber insurance should seek policies that contain language that includes coverage for employees that are using their own hardware outside of a business's physical workspace.

Businesses should also be aware of conditions in certain cyber insurance policies that must be followed, even while employees are working remotely, in order for the policyholder to be covered in the event of an attack. In the event of a cyberattack, some businesses may rush to shutdown their system to give their IT staff time to assess the attack and prevent further damage. However, some cyber insurance policies will not cover losses associated with voluntary shutdowns if the insurer determines such a shutdown was unnecessary or against best IT practices. As such, businesses should be careful to fully assess their options before instituting any voluntary shutdown of the systems.

In addition, some cyber insurance policies may require the insured to maintain certain security features, run regular security maintenance, or conduct regular inspections of the insured's cybersecurity systems. Businesses must be aware of such clauses in cyber insurance policies and ensure that their IT department continues to follow them even if employees are using their own hardware or programs that are not typically used while working from a business' normal workspace.

It remains to be seen what long term affects COVID-19 will have on workplaces across the country and what impact those changes will have on cyber insurance policies. Some experts are already predicting that many businesses will allow employees increased freedom to work remotely which will force cyber insures to amend their policies to specifically address coverage for employees that do not use hardware or networks directly provided or controlled by the insured business.

If you have questions regarding cyber insurance, feel free to contact Ariel E. Ronneburger at (516) 296-9182 or via email at aronneburger@cullenllp.com, Roxanne Tashjian at (516) 357-3704 or via email at rtashjian@cullenllp.com or Ryan Soebke at (516) 357-3784 or via email at rsoebke@cullenllp.com.

Practices

- Cybersecurity and Data Privacy

Attorneys

- Ariel E. Ronneburger
- Roxanne L. Tashjian
- Ryan M. Soebke