Rethinking Your Cyber Insurance Needs as Your

Digital Media and Data Privacy Law Blog
By Will Quick on 01.28.2022
Posted in Cyberattack, Data Breach, Data Security

The past 20 months have created a lot of transitions in how people work. Some companies still have the majority of their employees working remotely and intend to keep it that way permanently. Other businesses have tried to come back fully in-person only to send workers home again as new variants emerge and COVID cases begin to rise again.

We have seen an increase in cybersecurity incidents with such a dispersed workforce. Changes in working conditions, home systems that are less secure, and the general stress we are all under as the pandemic drags on have all likely contributed.

A survey released by Deloitte in October found that 98% of C-suite executives had come across at least one cybersecurity incident in the past year and 86% of U.S. executives had noticed an increase in attempts. However, the same survey found that 14% of executives said their company had no plans in place to either defend against an attack or respond to an incident.

One key piece of that incident response should be cyber insurance. Depending on the specific policy, “cyber insurance” can cover the cost of business disruption, lost revenue, equipment damages, attorney fees, forensic analysis and the expenditures associated with legally required notifications of the data breach. As with other types of insurance, thinking through your risks and knowing what type of cyber insurance coverage will be the most helpful should be an important part of your yearly planning.

A report issued in May by the U.S. Government Accountability Office (GAO) found that only 47% of businesses had cyber insurance in 2020. This is a significant gain from 2016, when the number was 26%, but it surprises me to read that a majority of businesses still do not have a financial safety net to help cover the costs of ransomware and other cyberattacks when those incidents make headlines month after month. I have to believe owners at those businesses believe that “it can't happen to us,” but they would be wrong. I handle security incidents for clients of all sizes and types and across industries ranging from food processing and manufacturing to transportation companies to financial institutions.

As people continue to work remotely, those businesses without cyber insurance need to look into it and those with cyber insurance need to check their policies to make sure they meet the needs of the current workforce and working conditions. For example, I recently dealt with a situation
where, when a company transitioned to remote working, it did not have enough devices to send each employee home with a computer, so it equipped the personal computers of some individuals with the software they needed for work. One of those personal computers was then hacked, opening the entire company system up to a data breach. However, the cyber insurance policy only covered devices owned by the company and so the business was forced to pay for the entire cost of the response, including my services. Look for important exclusions like that when reviewing your policies.

When reviewing cyber insurance policies, it’s important that a company’s IT department is involved in the process to make sure the policy captures all of the likely risks and exposure a company faces, as well as reflects the current working situation. A review by an attorney may also help identify possible red flags or exposures that are not covered by an insurance policy.

The GAO study cited above found that the increase in cyberattacks led to an increase in insurance costs, with premiums rising as much as 30% for some companies in 2020, at a time when insurers were also reducing coverage limits for some of the most at-risk industries, such as education and health care.

Many companies also think that one cyber insurance policy will cover all of their potential exposure. However, we are seeing an emerging trend of insurance companies issuing specific policies or riders for each possible risk and pricing those based on a particular businesses likely exposure. To help determine the appropriate pricing, or even if they will issue a policy at all, many cyber insurance companies are also requiring an audit of a company’s computer systems, data policies and other protections before issuing insurance – similar to how an individual might need a physical to get life insurance. Again, involving an attorney in this process can help determine your legal risks and exposures, as well as your technical ones.

Cyber attacks will likely continue to rise in 2022, but with proper precautions, companies can limit their financial and legal exposure and ensure they are better prepared for whatever threats may develop.