February 5, 2020

Cyber Insurance – Are You Covered?

By Joseph M. Ruscak

Over two-thirds of all businesses and organizations have had at least one cyberattack in the last two years, with half of those attacks targeted at small businesses. When these attacks hit, businesses may believe they have adequate protection against cyber risks, including risk management protocols and insurance programs in place. Unfortunately, with cyber insurance policies currently evolving in the market place, it is difficult to determine if a company has the adequate insurance coverage for a data breach, ransomware attack, or fraudulent wire transfer. Understanding your business's risks of a cyber-attack, the nature of the potential attack and the potential damages that could flow therefrom, is critical in ensuring that your business has the correct type and amount of cyber insurance.

Due to a lack of preparedness and general understanding, stories are commonplace where a company experiences a cyber event only to be followed by a swift denial of cyber insurance coverage. The best time to find out you need additional coverage, or a particular type of coverage, is obviously before you suffer an attack. As the new year begins, now is the time to take the appropriate steps to protect your business as best you can. This determination should be made in conjunction with an insurance professional, your internal IT expert, your risk managers, and those well-versed in the legal aspects of a cyber-attack.

First, if you are questioning whether you have cyber insurance, you probably do not. Cyber events are common exclusions to standard general liability policies. Typically, an additional policy or a specific rider is needed for cyber-event coverage. You should work with an insurance agent who is well versed in the cyber world, understanding the risks to your company and the insurance products on the market. Ask your agent: What exactly is covered? Is the insurance product offered intended to protect your business against your likely cyber risks? These determinations should be made in conjunction with your CISO, internal IT expert, or risk manager, as they will be better versed in your cyber and data privacy needs.

Once an insurance product is recommended to you, analyze it carefully for questions such as: What is excluded in the policy? What other limitations exists in the policy language? These exclusions, when read in the midnight hours of a cyber incident, may provide significantly less coverage than originally thought. For example, exclusions or policy limitations that deny coverage for wire fraud, man-in-the-middle attacks, ransomware and/or phishing are common. A cyber event could occur with the hacker requesting a fraudulent wire transfer and the unsuspecting insured complying. What was thought to be covered could easily be excluded, or cyber coverage could be denied and shifted to a sublimit under another category of loss (for example criminal act coverage). Another policy shift might include considerably higher deductibles for cyber-related events.

Often, the policy only covers cyber-attacks and unauthorized activity, and fails to cover accidental errors or omission. In other situations, human errors, including those of your own employees, are not covered. Unfortunately, during an attack, human and accidental errors are exactly what hackers exploit to their advantage. As such, lack of coverage in these areas can leave you quite vulnerable.

As you assess your future insurance needs, ask yourself the following questions: What are your needs and, specifically, what are your data needs? What kind of information are you holding, and what risk does it present? Can you financially weather a one-week shutdown of all your systems with limited or no access to your key business data? Can you afford to have your entire business rebuilt from back-ups? Finally, if you process payments or retain private information belonging to your customers, are you prepared to manage a breach involving the required public disclosures? Most businesses likely cannot weather this storm without significant insurance protection and a predefined incident response plan.

Assessing risk, exposure and a response plan in the cyber realm is complex and multifaceted. It often involves competing business priorities, hard to quantify risks, and legal landmines that remain hidden until an incident occurs. Cyber insurance may be an avenue to soften the blow to these risks, but only if it is well researched and the correct type of coverage is purchased. Our Cybersecurity and Data Privacy team, in conjunction with your risk manager, IT expert, and insurance agent who specializes in identifying your business risks and insurance coverage needs can help when its needed most, which is before a cyber incident.

Please contact us for more information about how we can partner with your team to assist you in the potentially daunting evaluation and to learn more about the other services offered in our Cybersecurity and Data Privacy Practice Area.

Joseph M. Ruscak
330.849.6716 | jruscak@ralaw.com

Chad L. Mowery
330.849.6782 | cmowery@ralaw.com

Megan Faust
330.849.6617 | lfaust@ralaw.com

E. Mark Young
216.820.4210 | emyoung@ralaw.com

Jeffrey J. Farkas
330.849.6673 | jfarkas@ralaw.com

This alert is informational only and should not be construed as legal advice. ©2020 Roetzel & Andress LPA. All rights reserved. For more information, please contact Roetzel's Marketing Department at 330.762.7725