Cybersecurity Awareness Month – Understanding the Complexities of Cyber Insurance Coverage

Many traditional liability insurance policies have exclusions for cyber-related risks and stand-alone cyber insurance policies are the norm to cover cyber liabilities. Still, cyber insurance policies are not standardized to the same extent as traditional liability policies are, so businesses need to be aware of the key issues when obtaining cyber liability coverage.

Cyber liability is difficult to quantify. The liability risk depends on, among other things, the nature of the business operations, the company's network security policies and infrastructure, and the types of data the company collects and stores. The key information needed to assess cyber liability risk is collected in the insurance application, which becomes part of the terms of coverage and false statements in the application could void the insurance. So, the first basic rule in cyber insurance is to pay careful attention to the information submitted in the application.

When issued, comprehensive cyber insurance policies cover first-party risks (i.e., damage and loss incurred directly by the insured) and some third-party risks (i.e., the insured causing potential liability to third parties). First-party coverage typically includes coverage for: (1) costs to respond to a cyber-incident including post-incident forensic investigation and data retrieval and restoration; (2) breach notification to comply with statutory and contractual obligations; (3) credit monitoring and identity theft protection services; and (4) reputation management through public relations and communications.

Third-party risks are liability that may arise from contractual obligations to indemnify or from litigation settlements or judgments from claims made by third parties due to the cyber breach. It is important to note that not all policies cover litigation costs. A cyber policy that covers litigation defense will mitigate the costs of defending what could be a large number of private actions stemming from a breach.

Many policies exclude coverage for government-issued fines, penalties and/or payment of ransom in response to a ransomware attack. Certainly, governmental fines and penalties can be costly, but the going rate of a ransomware attack could catapult the cost of a data breach from six figures to seven with the stroke of a cybercriminal's hand on a keyboard. Thus, it is imperative to work closely with your cyber insurance broker to understand the extent of coverage and what landmines exist in policy exclusions.

Cyber insurance policies are also typically written as "claims-made" or "occurrence" policies. Claims-made policies require that claims for coverage under the policy must be made during the period the policy was active and in effect. Occurrence policies are triggered by an occurrence during the policy period, regardless of when the claim is made. Since a "data or cyber breach" can be difficult to detect and may go undiscovered for some time, businesses should pay careful attention to the precise terms of when claims are covered and the requirements for notifying the insurer.

Even more challenging for organizations of late is that the cyber insurance market is in a state of flux. Cyber attacks are occurring with increasing frequency and the losses for each attack are steeply rising.

IBM's Cost of Data Breach Report estimates that the average cost of a data breach was a staggering $4.35 million in 2022.

As the demand for cyber insurance is rising, premiums are rising as well. The rise in premiums due to increased demand is also being fueled by the large payouts cyber insurance companies have made over the past few years. According to a Marsh report in 2021, cyber premium rates had increased 174% compared to the prior 12 months. Many are forecasting that companies could experience up to a 300% increase in premiums in the next few years.

Finally, the demand for insurance is exceeding the capacity of many cyber insurance companies that have tapped out their risk exposure under their policies. The National Association of Insurance Commissioners reports that the number of written cyber insurance policies increased by 21.3% from 2019 to 2020. Reinsurance capacity is scarce, and reinsurers have become wary of the large losses resulting from cyber attacks in many industries. There is some hope that the increased premiums will attract more insurance capacity, but it may take some time for the premiums to make up for the large payouts insurers have made.

These market factors are producing new business models in the industry. New cyber insurance companies are entering the market who are providing cybersecurity services along with the insurance product. The cybersecurity services help both the customer and the insurance provider proactively manage the risk of a breach from occurring.

When obtaining cyber insurance, whether it is a new policy or the renewal of an existing policy, a business should be prepared to show that their cybersecurity program, including their policies and procedures, are robust enough to satisfy the due diligence of a cyber insurance provider. In response to high premiums and coverage limitations, companies should work closely with their brokers to assess their appetite for risk in light of the sensitive information they collect and store.

It will be a bumpy road in the cyber insurance market for the next few years. Those businesses that are proactively anticipating the impact of the changes in the industry will inevitably fare the best.

For more information regarding cybersecurity insurance coverage, contact Jessica Copeland, Gail Norris, Mary Moore or any attorney in the cybersecurity and data privacy practice.

BOND SCHOENECK & KING ATTORNEYS