PKF O'CONNOR DAVIES
ACCOUNTANTS AND ADVISORS

Effectively Leveraging Cyber Insurance to Safeguard Against Threats

By Minesh Pandya, Director and Thomas J. DeMayo, Partner

In today's increasingly interconnected digital world, the rapid growth of different types of technology has led to an increase in vulnerabilities and threats resulting in business risks. Cybersecurity insurance has emerged as an important tool to help mitigate the financial and reputational impact of ever evolving and sophisticated cyber threat actors by transferring some of the risk to an insurer.

While this has led to a significant increase in the demand for cybersecurity insurance policies, the insurance industry is struggling to keep pace with the sheer losses being incurred as a result of incidents being paid. Once it was a simple process to obtain coverage; that is no longer the case. Similar to obtaining a quality life insurance policy, the underwriters want to know your cyber health before they provide the coverage. This is accomplished through lengthy questionnaires and, in some cases, external vulnerability scans.

In this article we explore some of the advantages and disadvantages businesses should consider when using cyber insurance to counter the rising tide of cyber threats.

Advantages of Cybersecurity Insurance

Financial and reputational protection is perhaps the most obvious benefit for businesses in the event of a cyberattack. The insurance can cover various costs associated with a cyberattack, including ransomware demands, legal fees, notification expenses, public relations efforts, forensic investigations, loss revenue and potential regulatory fines.

Additionally, many cyber insurance policies include pre-negotiated access to various service providers – often called the "panel" – which will be critical in mitigating some of the potentially negative results of a breach. These service providers range from cybersecurity incident responders to contain and remove the threat, legal counsel to navigate the increasingly complex maze of regulatory response requirements and potential litigation, public relations experts to minimize the reputational impact and service desks that facilitate credit monitoring for the victims of the incident.

Having access to this panel of experts helps to simplify the incident response process. A call to a single hotline number can put into motion a range of specialists who would otherwise require separate and disparate communications and, in some cases, retainers. While these responders will be crucial in resolving the incident at a surface level, separate external specialists are often called upon by businesses to perform complex root cause investigations and remediation activities. The panel providers are there to stop the bleeding, but in many cases are not the ultimate cure.

Downside of Cybersecurity Insurance

The biggest drawback of cybersecurity insurance policies is coverage limitations and exclusions. Policies vary significantly in their scope and coverage and certain types of cyber incidents, such as nation-state attacks or acts of war, may be excluded from coverage.

The use of the act of war exclusion by insurers has resulted in legal disputes, with businesses often challenging how the exclusion applies. One example is the case of the infamous NotPetya cyberattack in June 2017 against global biopharmaceutical company, Merck, in which the U.S. government attributed the attack to the Russian government. The attack cost Merck over $850 million worth of damage and disrupted the production of its HPV vaccine. At the time Merck's insurers, Ace American, denied coverage for the cyberattack citing exclusions based on "hostile" or "warlike" actions. In 2018 Merck sued Ace American for failing to pay out. A legal dispute ensued for five years and, more recently in May 2023, the New Jersey Superior Court Appellate Division issued a ruling in the case. The court found that the insurers had failed to demonstrate that the attack was a warlike action and affirmed the lower court's finding that the insurance companies had to pay.

In addition to act of war exclusions, policies may have limits on the amount of coverage available for different types of losses, such as intellectual property theft or business interruption. Recently, we have noticed policies being issued with coverage limitations on ransomware payments as well as a tiered payment structure if the breach was a result of vulnerability that was known to have existed for a certain period of time but was never patched. For example, if the business is breached as a result of vulnerability that was well known in excess of 180 days, the policy may not cover the loss. The insurance providers are implementing these conditions in order to ensure businesses have adequate "skin in the game" and ensure their cybersecurity programs are being consistently maintained and matured.

Cyber Insurance Questionnaires, Coverage and Claims

As the questionnaires have lengthened exponentially, so has the opportunity to answer incorrectly, falsely claiming the existence of a control. While larger organizations may have many skilled resources to call upon to ensure the questions are answered in the context they are intended, many small to medium businesses do not have that same level of advisement. This results in answers being provided by those not qualified to answer or those afraid to answer truthfully. Failure to answer correctly could result in non-payment if the breach was the result of a control attested to as existing.

A separate issue is that we often find our clients struggling to answer the questionnaires because the questions are worded in a very binary capacity, meaning it exists or it doesn't. In an operating business, such clearly delineated lines don't exist. In many cases, the answer depends on the risk and the circumstance. In these situations, we advise or assist our clients in writing out supplemental responses that clearly explain the control as is to ensure the underwriters have the facts and the business is truthful and transparent.

Cybersecurity insurance itself can be expensive, especially for businesses with higher risk profiles or those operating in industries prone to cyber threats. Premiums are based on factors such as the organization's size, industry sector, security controls in place and previous cyber incidents. As with life insurance, the more weakness you have, or unhealthy you are, the more you will pay for coverage. As of late, many insurers will simply not quote a policy if your responses or their external investigations of your security posture evidence red flags. Certain controls have become non-negotiable such as Multi-Factor-Authentication (MFA) for remote access.

Setting up the policy itself and then making a claim can be a complex and time-consuming process. The process of invoking cyber insurance should be well embedded into your incident response plan. If you have coverage, and you act without invoking the coverage correctly per the policy, you risk the claim being denied. For example, if you rush to pay the ransom out of urgency and fail to include the insurance provider in deliberations, there is a good chance you will not be reimbursed in full or at all. Businesses should be prepared to invest technical and business resources and work closely with insurers during the set-up and potential claims process.

Conclusion

It must be emphasized that relying solely on cyber insurance as a risk management strategy can create a false sense of security. While insurance can provide financial and reputational protection, it does not

prevent cyberattacks or guarantee the absence of reputational damage. Cyber insurance should be seen as a complement to a comprehensive cybersecurity strategy rather than a substitute. Reviewing the specific cybersecurity risks in your business operating environment and ensuring that your cybersecurity insurance policy provides adequate coverage for these risks is a sensible approach.

During the procurement process, it is crucial for businesses to carefully review and accurately respond to the questions being asked regarding your cybersecurity program. Should you be quoted, the insurance policy terms and conditions need to be further evaluated to understand the terms, limitations, exclusions, and to ensure it aligns with business objectives and overall risk appetite. This should be achieved by working with legal, technical and business management teams alongside the insurers themselves.

Our assessment and program development methodologies are designed and focused to help minimize the likelihood of needing to invoke the insurance coverage; however, in the event it is needed, we can help ensure your incident response plans are comprehensively designed to facilitate recovery.

Contact Us

At PKF O'Connor Davies, we not only know the technical risk, but we understand and can effectively communicate the resulting cyber risk. If you need assistance in developing a cybersecurity program that is effective and aligned to your risk, please contact your client engagement team or either of the following:

Minesh Pandya
Director
Cybersecurity and Privacy
mpandya@pkfod.com | 212.867.8000

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Partner
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com | 646.449.6353