Sills Cummis & Gross P.C.

Client Alert Cybersecurity

Transferring Cybersecurity Risk: Considerations When Obtaining Cyber Insurance

While procuring cyber insurance is an increasingly important business decision, choosing cyber insurance is not a simple process of merely identifying the amount of coverage desired and then paying for the corresponding premium. Instead, as set forth below, it presents a matrix of considerations to be explored to ensure receipt of appropriate coverage when needed.

The Importance of Cyber Insurance

In the face of continued and more destructive cyber threats and the advent of more demanding statutory and regulatory requirements, it is critical for a company not only to mitigate risk through comprehensive cybersecurity management but also to transfer that risk by obtaining tailored cyber insurance. Indeed, more rigorous regulations, along with their attendant financial penalties for noncompliance (such as the EU's General Data Protection Regulation ("GDPR"), which became effective May 25, 2018, or the NY Department of Financial Services ("NYDFS") cybersecurity regulation, which was instituted in 2017) are likely to become the norm, not the exception. Violation of these more recent rules and requirements (and potential expenses and related fines) also do not apply only when data is lost through an actual breach, but also when data is destroyed or cannot be accessed (ransomware) and when data is improperly collected. Moreover, cyber risks and costs are indiscriminate and affect all industries.

May 2018

Client Alert Cybersecurity

To offset these serious risks, cyber insurance usually is necessary. Third-party cyber liability claims are not covered under most general liability policies including the Insurance Service Organization's industry standard GL form. Director & Officer liability policies usually exclude cyber liability claims. Property policies, including the ISO "All Risk" form, typically exclude first party cyber claims. Limited first party cyber coverage may be available through crime policies, and some Information Technology Industry Errors & Omissions policies afford third party cyber coverage. In most cases, however, only a cyber policy can assure a company of the desired coverage. A company has a much better chance for coverage and a prompt resolution of its claim under a cyber policy without the need to resort to litigation.

While cyber insurance has been available since the late 1990's, it is rapidly expanding because of the continued need for a holistic approach to cybersecurity protection. Indeed, insurance companies expect a surge of business as companies rush to purchase cyber insurance following the arrival of tougher regulations like the GDPR.

Cyber security and liability risks also often involve highly-technical, rapidly evolving information technology issues. A prospective insured should inquire regarding the cyber experience of its broker, particularly if it is not using a large multi-line producer who has access to an IT consultant or cyber specialist. Some brokers specialize in cyber insurance, and an insured should consider using a broker who possesses cyber experience. While "bare bones" cyber coverage is available from authorized or "admitted" insurers, more comprehensive niche cyber coverage often is available only in the surplus lines or "non-admitted" market and can be brokered only by surplus lines producers.

The selection of an insurer is even more important. In addition to issues of Best's Financial Quality and Size Ratings, many insurers offer low cost, bares bones third-party coverage, while other insurers offer broader, albeit more expensive, coverage, and better claim service.

Cost-wise, premiums will be lower for those companies with comprehensive cyber-risk management plans in place with demonstrated levels of security and internal controls, i.e., better security equals lower risk, which equals more competitive pricing. A company therefore is further incentivized to ensure it has adequate procedures in place to prevent, detect, investigate, and report data breaches.

The Level of Coverage Needed: Initial Considerations

One of the most important steps in the process of obtaining cyber insurance is to determine what type of coverage a company needs based on reasonably anticipated

cyber risks inherent to a company's business and position in the marketplace. There are multiple considerations a company should undertake in assessing the kind and amount of coverage needed.

What type of company are you?

A company should consider:

- its industry and the type of services it offers;
- the type of data it handles (e.g., financial information, health information, credit information);
- the makeup of its customers (e.g., whether they include EU citizens); and
- what regulations it must follow.

Depending upon the kind of data it collects and handles, the company will be subject to a different array of regulations, which should inform the company regarding the type of cyber insurance coverage to be sought. If a company is a financial institution, it must comply with the privacy rules of the Gramm Leach Bliley Act. If the company handles personal health information, it will be subject to the privacy requirements of the Health Insurance Portability and Accountability Act, HIPAA. If the company handles the data of EU citizens, it will be subject to the privacy restrictions (and severe potential penalties) of the GDPR.

First-Party and Third-Party Costs

The company also should think about the kinds of costs it may incur to manage a cyber incident/breach and whether cyber insurance coverage to defer or recoup all of those costs is necessary or prudent. Such first-party costs can include:

- **forensic investigation costs** to determine the source of the cyber incident/breach and the extent of harm caused
- **remediation costs** to rectify any network problem or software deficiencies
- **notification costs** to customers whose data was compromised
- **data restoration costs** of data stolen, lost, or altered
- **business interruption costs** to help restore business functions and to maintain business capabilities while responding to a cyber incident
- **legal costs** to evaluate regulatory obligations and assess any liability
- **public relation costs** to help maintain and/or restore confidence in the company

Client Alert Cybersecurity

Considering these first-party costs, however, is not as straightforward as it may seem. For instance, assuming a company wants a policy to cover notification costs to advise its customers of a data breach, a company still needs to determine the type of notification it envisions. Does it merely want to comply with statutory notification requirements or might it want to take a more aggressive approach to notification for customer relation purposes? And how is the company going to notify its customers? Email? Regular mail? First Class mail? Similarly, when assessing remediation costs, the company also needs to determine if it wants to provide credit monitoring to its customers and have those costs covered under a cyber policy. A company must think through these issues to help ensure the right cyber insurance coverage is obtained.

Furthermore, a company may also incur third-party costs as a result of a cyber-event, such as defending against a litigation or regulatory action. Contemplating cyber coverage for these types of third-party costs also compels additional considerations regarding the extent of coverage desired. For example, legal fees in defending a claim often can approach or even exceed the ultimate cost of settling the claim. A company should decide if it wants its litigation costs to erode the policy's limit of liability, sometimes referred to as being "cost-inclusive," or whether defense costs should be in addition to the limit of liability. With regard to a regulatory inquiry, while payment of fines and penalties is unlawful in some jurisdictions and is often excluded from coverage, the company must determine if it wants coverage to include investigatory costs in responding to the governmental inquiry. Some policies cover up to half of the investigatory costs of responding to a governmental inquiry or subpoena, usually subject to a sublimit on liability.

Do the Provisions of the Policy Ensure the Desired Coverage?

Once a company identifies the coverage it hopes to purchase, it then is essential to carefully consider the specific provisions of a cyber policy to ensure receipt of the level of coverage sought for the cyber risk possibilities reasonably envisioned. Among the questions when analyzing the policy's provisions are:

> **When is coverage triggered?**

- Is the policy written on an "occurrence" basis, i.e., the breach must occur during the policy period to be covered, or is it written on a claims-made basis, i.e., the claim must be made and reported during the policy period in order for coverage to be available?
- If the policy is written on a claims-made basis, does the breach nevertheless have to occur during the policy period, does it merely have to be discovered in the policy period, or both?

- Is intentional conduct required (by a third-party or malicious company insider) or can coverage be triggered by the negligence of an employee?
- Is the conduct of a malicious insider to the company covered or must the cyber incident be caused by an outside third-party?
- Must data have been disseminated outside the company (a breach) or will the policy also cover situations where data is destroyed or cannot be accessed (e.g., ransomware)?

> **What kind of information is covered?**

- How is "personal information" defined?
- Is "confidential corporate information" covered?

> **Does the policy require minimum security requirements be maintained to protect the company's computer network and data?**

> **What devices are covered?**

- Are only the company's servers and computers covered?
- How are mobile devices (laptops, mobile phone, thumb drives) treated?
- If the company allows employees to use personal devices or work remotely (BYOD – Bring Your Own Device policies), are cyber incidents originating on an employee's personal device covered?

> **Are cyber breaches or incidents caused by vendors assisting the company (e.g., HVAC, data processors, cloud providers) covered?**

- Would coverage only extend to breaches caused by a vendor on the company's network?
- Would coverage extend to a breach of a vendor's network housing the company's data?

> **What are the policy provisions regarding notice and defense of a claim?**

- How quickly does the policy require a claim to be reported to the carrier?
- Whose knowledge of a breach is imputed to the company for the purpose of determining whether a claim has been reported late and whether an exclusion applies?
- Does the definition of "claim" include responding to a subpoena?

- Is the defense obligation of the policy a "duty to defend" where the insurer controls the defense and settlement of a claim or does the policy have a duty to advance defense costs, which permits the policyholder to control the defense and settlement of the claim at the cost of the insurer?
- If the policy has a duty to advance costs, are there limitations on who the company can retain as outside counsel or as a forensic expert?
- Are regulatory investigations covered?
- Does the policy cover investigatory costs in responding to a governmental inquiry?
- Are fines covered? If so, is the company domiciled in a jurisdiction where indemnification against fines and penalties is not against public policy?
- How is regulator defined? Does it cover EU regulators?

To be sure, disputes between policyholders and insurance carriers are inevitable, and insurers will attempt to strictly construe policies against coverage. Courts are just beginning to interpret cyber insurance policy provisions, sometimes coming out on opposite sides of the same issue depending upon the jurisdiction.

For instance, courts have disagreed whether cyber insurance policies cover losses resulting from social engineering, i.e., when a company employee is falsely manipulated to wire out company funds based on what is believed to be a legitimate email authorizing the transfer but what is actually an email initiated by a fraudster. Insurers may assert that a loss caused by social engineering (also known as business email compromise) is not a direct loss under the computer fraud provisions of a cyber insurance policy. Carriers attempt to distinguish between fraudulently causing a transfer (via social engineering) and causing a fraudulent transfer (via hacking into a company's computer network to wire out funds).

Insurers also have sought to disclaim coverage by invoking exclusions for a company's failure to maintain agreed-upon levels of cybersecurity to protect the company's network and data. Courts have been asked to construe cyber policy provisions to determine whether the insured satisfied the policy's security requirements. Considering that industry cybersecurity measures are constantly updated, a company should attempt to avoid a situation where a court's interpretation of policy language and evaluation of a company's cybersecurity efforts will determine whether it can recoup losses from a cyber event.

Client Alert Cybersecurity

Conclusion

As criminals find new and more inventive ways to attack computer systems or fraudulently cause the theft of company funds, a company faces the increased risk of loss, which can result from a combination of illegal activity, imperfect network security, and employee negligence. As such, a company should undertake a complete strategy to combat cybersecurity-related threats, which includes procuring appropriate insurance coverage to manage reasonably anticipated cyber risks. Carriers may attempt to dispute claims, so a company must give special attention to cyber policy language to avoid the possibility of coverage being denied. To help negotiate policy provisions to avoid ambiguities and potential grounds for disputes, a company should explore using an insurance professional to help negotiate a policy with the desired coverage, including identifying additional policy endorsements that may be available to cover certain specific cyber threats. When procuring cyber insurance, considering the questions and issues outlined above may make the difference between receiving expected cyber coverage and not.

If you have any questions regarding information in this alert, or if you need more information, please contact the following Sills Cummis & Gross attorneys:

Joseph B. Shumofsky, Esq.
Chair, Cybersecurity and Data Privacy Group
jshumofsky@sillscummis.com | (973) 643-5382

Thomas S. Novak, Esq.
Chair, Insurance and Reinsurance Group
tnovak@sillscummis.com | (973) 643-5383