Data Breach Risk Management: Keeping Up With Evolving Cyber Liability Insurance

New York Law Journal
October 15, 2018
By Nadira K. Kirkland, Esq.

Just as cyber threats are continually evolving, so are cyber liability insurance policies. With data breaches a common occurrence, many companies are focusing on their IT systems, but tend to overlook the insurance aspects. When preparing for and responding to a cyber event, having comprehensive insurance coverage is critical. Personnel responsible for detecting, reporting and responding to cyber events and privacy violations should also have a thorough understanding of the coverages provided under their cyber policies and how those policies are triggered – well before an incident occurs.

The Evolution Begins

In the past, companies and businesses have sought coverage under traditional types of policies, such as property or commercial general liability (CGL) policies. However, there has been extensive litigation over when and in what circumstances a CGL policy covers a data-breach claim. Beginning in 2001, CGL policies began excluding "electronic data" from coverage and in 2014, additional exclusions emerged in CGL policies that were designed to eliminate coverage for cyber-related damages.

About 25 years ago, technology companies bought errors and omissions (E&O) insurance with the Y2K threat. Over time E&O policies were extended to include unauthorized access to a client system, destruction of data or a virus impacting a customer's system. The technology coverage, often called "network security" or "Internet liability" was an add-on to the existing policy. Five to ten years ago, these "network security" policies expanded into the privacy space by providing clear coverage for breaches of confidential information. Once coverage expanded, financial institutions, retailers and other companies holding considerable consumer data, but who were not providing the type of technology services that would warrant buying E&O insurance, took notice and began looking into stand-alone policies.

Lots of Jargon But Four Common Components

The term "cyber" coverage can vary with companies and groups. Generally, cyber liability insurance covers financial losses that result from data breaches and other cyber events. Many policies include first-party, third-party or both coverages. First-party coverages apply to losses sustained by the company directly. First-party coverages are often subject to a deductible. Third-party coverages apply to claims against the company by people who have been injured as a result of the company's actions or

inactions. Virtually all cyber liability policies are claims-made.

Although various insurance companies use different names and terminologies, cyber coverage insurance is some combination of basically four components: E&O, media liability, network security and privacy. These categories are sometimes conflated or further divided into other subparts.

As noted above, E&O covers claims arising from errors in the performance of services, which can include technology services such as software consulting or more traditional professional services such as attorneys, medical personnel and financial planners. This is a first party claim.

Media liability is a third-party claim pertaining to advertising injury such as infringement of domain name, intellectual property, copyright/trademark infringement and defamation, libel and slander. Due to the presence of businesses on the Internet, companies have seen this coverage migrate from their general liability policy to being bundled into a media component in a cyber policy or even a separate media liability policy.

Network security is both a first- and third-party claim. A failure of network security can lead to many different exposures, including a consumer data breach, destruction of data, virus transmission and cyber extortion. Network security coverage can also apply to trade secrets or improper access to information contained in patent applications.

Privacy is also a first and third-party claim. It includes the wrongful collection of personally identifiable information (PII), which usually pertains to medical, health and financial records. PII is defined in some regulations/statutes but there is not a standardized definition, especially in the U.S., so insurers may specifically define PII depending on the company's business model.

Cyber coverage includes some of the following first-party costs when a security failure or data breach occurs:

- Legal advice to determine notification and regulatory obligations
- Notification costs
- Forensic investigation of the breach
- Offering credit monitoring to customers as a result
- Public relations expenses (also referred to as Crisis Management)
- Business interruption, loss of profits and extra expense during the time that your network was down (property policies cover income losses and extra expenses that result from an interruption in business operations caused by physical damage to the covered property, which does not include electronic data)

Cyber coverage includes some of the following common third-party costs:

- Legal defense
- Cost of responding to regulatory inquiries
- Settlements, damages and judgments related to the breach
- Liability to banks for re-issuing credit cards

- Breach related fines imposed by the state or federal government. With the European Union's General Data Protection (GDPR) wide range of mandates and steep fines, some violations of GDPR may not be covered.

Usually Not Covered

Cyber liability insurance has more comprehensive coverage than a CGL or standard E&O policy; however, cyber liability insurance does not cover:

- Loss of future revenue
- Reputational harm
- Diminished value of intellectual property
- Costs to improve internal technology systems

Insurance frequently excludes losses or claims attributable to intentionally dishonest or criminal acts, breach of contract, theft of trade secrets, unfair trade practices and employment practices and cyber liability insurance is no exception. A determination that a loss arose out of an intentional act might eliminate coverage. Also, the cyber liability policy could exclude coverage for failure to meet certain security rule requirements and failure of a third-party or cloud vendor to protect any data entrusted to it.

Claims-Made Policy

Understanding the terms of the insurance policy is just as important as understanding when it is "triggered." Cyber insurance is claims made and the policy will have a discovery trigger. This means the policy can be used when the insured first discovers the event, regardless of when the act or acts causing or contributing to the loss occurred as long as the claim is made during the policy period. This is very important in cyber liability insurance because some companies do not immediately know when there has been a breach. The Ponemon Institute found that in 2017, it took an organization an average of 191 days to learn that a data breach had occurred. (Ponemon Institute Research Report, 2017 Cost of Data Breach Study, June 2017.)

The Evolution Continues

Any organization that stores and maintains customer information or collects online payment information, or uses the cloud, should consider adding cyber insurance to its budget. Also considering the proliferation of devices that now connect to business networks in a vastly global space, there are simply more opportunities for malicious access to an organization's assets.

Cyber liability insurance will not exonerate a company from maintaining a high level of overall security and does not take away the need to conduct the appropriate due diligence when dealing with outside vendors. But it can act as a source of funds and resources in the aftermath of an incident. Knowing how the cyber liability policy is positioned within other insurance coverages and understanding how to engage each one is important. In performing a cyber incident exercise, a review of how the insurance would or would not have been triggered would highlight any potential gaps in coverage. Since cyber liability insurance does not have a standard risk coverage form and terms and language vary from insurer to insurer

and policy to policy, it is imperative to speak with the broker to obtain an understanding of what is covered in the policy and individualized offering to meet the company's business model and goals.

The next wave of cyber liability insurance may address different gaps as technology continues to dictate the market and access to more data and information.

Nadira K. Kirkland is Special Counsel in the Casualty Department in the New York City office of Marshall Dennehey Warner Coleman & Goggin. She is a Certified Information Privacy Professional (CIPP/US) and a member of the International Association of Privacy Professionals (IAPP). She may be reached at nkkirkland@mdwcg.com.