Insurance Coverage Basics for Cyber Risks

Authors: Jennifer Thiem and Laura Musselman (K&L Gates - Charleston)

Scarcely a week goes by without a headline of some new cyberattack, be it against companies, nonprofits, or even U.S. cities and municipalities. Within the last several months alone, we've learned of several large attacks including the data breach of a large financial institution, which affected approximately 100 million customers in the United States. However, there has also been a rash of non-publicized attacks that can make a significant dent in a company's bottom line. According to the Privacy Rights Clearinghouse, there have been over 9,000 reported data breaches impacting over 11 billion records since 2005. Because insurers and victims are sometimes reluctant to disclose breaches due to reputational or competitive concerns, this number is likely underinclusive. As the number of attacks increase, so does the cost of responding. The Ponemon Institute reports that the average cost of a data breach to a company is approximately $4 million, with a significant amount of that spent on post-breach notification alone. Suffice it to say that this expense can be financially devastating to many companies.

Your organization is not immune. Reflect on the volume of personally identifiable information and personal health information your organization holds. Now consider the number of computers in your office, the number of your employees who carry smart phones, tablets, and portable storage drives. Given the prevalence of data breaches and the high costs associated with such breaches, organizations should examine their current insurance programs to determine what coverage may already exist and consider enhancing their existing coverage or filling any gaps through "cyber" risk policies.

Potential Coverage Under Traditional Policies

Most companies have commercial general liability ("CGL") insurance that may cover certain cyber risks. While coverage is ultimately dependent on the specific facts underlying the claim, the insurance policy, and the law, courts have upheld coverage for losses resulting from data breaches and other claims alleging violations of privacy rights. Not surprisingly, insurers have sought to limit their exposure by adding exclusions and limitations. The discussion below focuses on key coverage provisions in traditional insurance policies along with exclusionary language that seeks to curtail coverage.

CGL policies insure against liability to third parties as a result of operating a business. These policies typically include two coverage parts — Coverage A for bodily injury or property damage and Coverage B for personal injury and advertising injury. The discussion below highlights potential coverage under each of these coverage parts.

In a CGL policy, "property damage" is commonly defined as "physical injury to tangible property, including all resulting use of that property" and "[l]oss of use of tangible property that is not physically injured." Insurers have argued that electronic data is not tangible property that can

suffer physical injury. The 4th Circuit Court of Appeals agreed with the insurer in *America Online, Inc. v. St. Paul Mercury Insurance Company*, reasoning that "tangible" meant "capable of being touched" and "having physical substance apparent to the senses" and refusing to find tangible property coverage for damage for data and software.[1] Additionally, in response to other federal circuit's courts finding that tangible property *could* include electronic data, insurers have revised their coverage to expressly exclude "damages arising out of the loss of, loss of use, damage to, corruption of, inability to access, or inability to manipulate electronic data."

Under Coverage B, policyholders should review the definition of "personal and advertising injury" to determine whether cyberattacks may be covered. Under many policies, "personal and advertising injury" is defined to include "oral or written publication, in any manner, of material that violates a person's right to privacy." The issues in a coverage dispute under this definition would focus on whether there has been a "publication" that violates a third party's "right of privacy." In an unpublished opinion, the 4th Circuit Court of Appeals affirmed a district court opinion finding that publication occurs when information is "placed before the public," and therefore is triggered the moment records become accessible to the public, not only when a member of the public actually accesses the records.[2] Such interpretation could lead to a more expansive view of when "personal and advertising injury" coverage applies in the cybersecurity setting.

In 2014, the Insurance Services Office Inc. introduced a series of data breach exclusionary endorsements to both Coverage A and Coverage B. With respect to Coverage B, the new endorsements exclude "[p]ersonal and advertising injury arising out of any access to or disclosure of any person's or organization's confidential or personal information." Time will tell how this and other exclusions and limitations will be interpreted by courts.

Cyber Policies

Given the differing interpretations regarding the existence or non-existence of coverage under traditional policies as well as the insurance industry's efforts to curtail coverage under these policies, insurance companies have begun more forcefully marketing cyber policies. Cyber insurance is now generating $2–3 billion in annual premiums.

This new wave of insurance is specifically tailored to cover cyber risks; however, the marketplace for cyber coverage is not standard. Like traditional insurance, cyber policies can insure first-party and third-party risks, and coverage is also available for items such as regulatory liability and remediation costs.

Third-party liability coverage under a cyber policy may include losses resulting from a data breach, transmission of malicious code, or denial of third-party access to the policyholder's network and other security threats to networks including defense and indemnity costs associated with third-party actions against a company. Policies providing this privacy and network security coverage generally do not cover bodily injury or property damage; instead, this coverage part is focused on privacy and network security-related damages. Companies should evaluate whether their policies

[1] 347 F.3d 89, 94–95 (4th Cir. 2003) (applying Virginia law); *see also Sirona Dental, Inc. v. Smithson*, No. 3:14-CV-00714-RJC-DSC, 2015 BL 458059 (W.D.N.C. Sept. 29, 2015) (finding electronic data was intangible property while discussing a trespass to chattels claim); *WJ Global LLC v. Farrell*, 941 F. Supp. 2d 688, 693 (E.D.N.C. 2013) (finding electronic data was intangible property while discussing a conversion claim).

[2] *Travelers Indem. Co. of Am. v. Portal Healthcare Sols., L.L.C.*, 644 F. App'x 245 (4th Cir. 2016).

cover unintentional *and* unauthorized disclosures, as well as whether their insurer offers coverage for violation of privacy laws or failure to comply with the company's privacy policies.

Cyber insurance policies may also provide coverage for claims for civil, administrative, or regulatory investigations and proceedings. As with other regulatory liability coverage, a frequent point of contention between companies and their insurers for third-party liability coverage is when or how an administrative or regulatory investigation or proceeding is actually commenced. Accordingly, companies in the market for this particular type of coverage should review how coverage is triggered.

Additional third-party liability coverage may include:

- amounts payable in connection with Payment Card Industry ("PCI") demands for assessments for alleged non-compliance with PCI data security standards; and

- liability from claims alleging infringement of copyright and other intellectual property rights and misappropriation of ideas or media content, as well as torts such as slander, libel, and defamation.

First-party coverage under a cyber policy may include network or business interruption resulting from operations being disabled by a cyberattack. Companies should consider whether their network interruption coverage includes third-party system failures, cloud failures, or non-malicious acts. The waiting period and length of restoration period covered can also make a large impact on a company's recovery, depending on whether the insurance only covers the down time or also extends coverage while the business returns to its pre-event status.

Ransomware and other extortionist schemes have also led insurers to offer coverage for losses resulting from extortion, including payments of an extortionist's demand to prevent network loss or implementation of a threat and related expenses. Increasingly, ransom demands for electronic data may come not from private hackers but from state actors. For example, the U.S. Department of Justice indicted an Iranian hacker in 2017 for allegedly hacking into HBO's computer system and a North Korean programmer in 2018 for several high-profile cyberattacks, including the Sony Pictures Entertainment hack and the WannaCry ransomware virus. Policyholders should consider whether their coverage includes attacks from state actors, or whether those attacks are excluded as acts of war or terrorism.

Additional first-party coverage may include:

- response costs associated with post-breach remediation including notification requirements, credit monitoring, call centers, public relations efforts, forensics and crisis management; and

- the cost to recover data that are damaged by malicious code or stolen.

As noted above, policies are not standardized and indeed can be highly customized. Policies must be carefully analyzed relative to potential exposures. As with any insurance policy, coverage is dependent on the policy language as applied to the facts at issue.

D&O Policies Covering Cyber Risk

Now that cyber security is widely recognized as a boardroom issue, it is almost inevitable that senior management will receive some, if not much, of the blame for a resulting data breach.

In recent years, shareholders and consumers have brought a number of derivative and securities-related class actions against directors and officers for alleged failure to take adequate steps to prevent data breaches. For example, shareholders filed securities-related class action lawsuits against Equifax and its executives following its disclosure that it had sustained a data breach impacting more than 140 million customers. Until recently, most of these data breach shareholder lawsuits had been unsuccessful from the plaintiffs' perspective. In 2018 and 2019, however, Yahoo settled a data breach-related securities class action lawsuit for $80 million and a data breach-related derivative suit for $29 million. Additionally, in 2018 the U.S. Securities and Exchange Commission ("SEC") issued new cybersecurity disclosure guidance urging public companies to be more forthcoming when disclosing cyber risks and incidents. Together, these developments may lead to more shareholder lawsuits.

Directors and officers may also face liability under regulatory investigations or proceedings. In 2017, the SEC announced the creation of a new cyber enforcement unit, which (combined with the new guidance discussed above) could lead to more cyber-related enforcement actions. On the heels of the SEC's aforementioned new cybersecurity disclosure guidance, in 2018 the SEC levied a $35 million penalty against Yahoo's successor in interest, Altaba, for Yahoo's two-year delay in reporting its 2014 data breach. Altaba agreed to pay the penalty under a neither admit nor deny basis. Based on the SEC's heightened scrutiny of cybersecurity, directors and officers may also be personally exposed to regulatory enforcement action.

Directors and Officers ("D&O") insurance can help protect directors and officers against civil or regulatory liability, but standard D&O policies may not have been written with cyber and technology related risks in mind. Directors and officers should review their existing D&O policies and request changes aimed at maximizing coverage for cyber liabilities, where necessary. Such revisions may include adding coverage for claims not only by third parties, but by the company, liquidators, administrators, and shareholders. Directors and officers should also consider the wording of policy exclusions for dishonest or fraudulent conduct or claims arising from the provision of professional services to maximize coverage.

Conclusion

In this day and age, no organization is immune from cyberattacks. While traditional insurance remains a valuable asset, all organizations should consider purchasing cyber insurance, including cyber coverage under their D&O insurance. Before an attack, companies should evaluate and address potential vulnerabilities. Experienced counsel can not only assist with the analysis of the existing insurance program, but also help negotiate favorable terms and coverage to ensure no gaps or overlaps in coverage.

Jennifer Thiem is a partner in the firm's Charleston office. Her practice focuses on insurance and risk management counseling and complex commercial litigation. Ms. Thiem has counseled clients with respect to coverage or potential claims under a variety of insurance policies, including

general liability, directors and officers liability, professional liability, employers liability, representations and warranties and commercial property.

Laura Musselman is an associate in the firm's Charleston office, where her practice focuses on commercial litigation and white collar investigations and defense. Ms. Musselman has experience representing companies and individuals before the U.S. Department of Justice, U.S. Securities and Exchange Commission, and Public Company Accounting Oversight Board in connection with civil and criminal investigations.