Cybersecurity Law Report
An Acuris company

Lowenstein Sandler

December 4, 2019

CYBER INSURANCE

What Cyber Insurance Covers, What to Watch For and How to Get the Right Policy

By Eric Jesse and Jason Meyers, *Lowenstein Sandler*

While cyber insurance has become increasingly popular over the past several years, many companies still lack this protection. Companies without cyber coverage might look to their "traditional" policies, like general liability or crime, but coverage for cyber risks under those policies can be limited. Therefore, companies without cyber insurance should seriously consider securing it as part of their cyber risk management.

Additionally, whether a company has cyber insurance already or is considering purchasing it, it needs to understand the "fine print" that is often the difference between coverage or a denial. These are not "off-the-shelf" policies. Rather, cyber policies can be complicated, often with a laundry list of exclusions and defined terms (that can also limit coverage). Further, policy forms are continually changing as cyber insurers react to the threat landscape and insurance claims. Therefore, understanding – and negotiating – the scope of coverage and ensuring that it encompasses your company's risks is critical to maximizing the benefits that cyber insurance provides.

See "Choosing Cybersecurity Insurance in a New Risk Environment" (Nov. 6, 2019).

What Cyber Insurance Covers

Standalone cyber policies generally provide a hybrid of "first-party" and "third-party" coverages. The first-party coverage insures loss that insureds suffer because of a cyber incident. It generally includes the following:

- **Breach Response Costs.** When a data breach occurs, this coverage typically insures legal fees the insured incurs to understand its notification obligations; computer forensic costs to investigate the scope of the breach; and costs for notification to affected individuals, credit/identity theft monitoring and call service centers.
- **Business Interruption.** This coverage insures against lost profits and extra expenses (beyond usual business expenses) that a company incurs if a system failure impairs the company's ability to operate. Some policies also offer contingent business interruption coverage when the insured cannot operate because a vendor has suffered a cyberattack.

- **Cyber Extortion/Ransomware.** This coverage applies when a cybercriminal hacks into the company's computer system and threatens to damage data, introduce a virus or shut down access to the network unless a ransom is paid.
- **Cyber Crime.** Cyber policies may offer cyber-related crime coverage such as: (i) computer fraud (a criminal using computers to steal money); (ii) funds transfer fraud (a criminal tricking a bank into transferring funds from the insured's account); and (iii) social engineering (a criminal tricking the insured's employee into transferring money).
- **Data Restoration.** Policies with this coverage generally cover the costs to restore or replace lost or damaged data or software because of a cyber incident.

Cyber insurance typically provides the following types of third-party coverage, *i.e.*, coverage that insures against lawsuits, claims and/or proceedings brought against the insured:

- **Privacy and Network Security Liability.** This coverage insures against claims and lawsuits brought by plaintiffs due to the unauthorized theft or disclosure of sensitive data, unauthorized access to computer systems or denial-of-service attacks.
- **Payment Card Loss.** This coverage generally applies to insureds who handle credit card information that is stolen or accessed, and it covers the amounts they are liable to pay under the terms of a merchant services agreement with a credit card company/processor.
- **Regulatory Fines and Penalties.** When an insured is subject to a regulatory proceeding or an investigation because of a data breach, cyber policies can cover civil fines or penalties payable to the government or regulator (so long as such amounts are insurable under applicable law).
- **Media Liability.** Sometimes cyber policies cover media liability claims for acts such as libel, slander, defamation, copyright infringement, invasion of privacy and misappropriation of ideas.
- **Technology Services and Products.** For companies that are in the technology sector, some cyber policies can cover claims of errors and omissions as part of an insured's technology-related services or products.
- **Defense Costs.** The third-party coverages identified above also include coverage for a company's defense costs. Defense costs typically erode the policy's limit of liability.

Many of these coverages can be subject to sublimits that are less than the aggregate limit of liability. To avoid an unwelcome surprise when there is a cyber incident, companies must be aware at the outset of any sublimits and confirm that the sublimits are appropriate for their risk appetite. Often, sublimits can be increased by just asking the insurer or for an additional premium.

See CSLR's three-part series on using cyber insurance to mitigate risk: "From Assessing the Need to Managing Existing Policies" (Oct. 3, 2018); "Getting Savvy About Cost and Policy Terms" (Oct. 10, 2018); and "Policy Management and Breach Response" (Oct. 17, 2018).

Cautionary Tales From the Courts

Insurance programs are patched together with more parts now than ever before, but as court cases have shown, standalone cyber policies must be one of those parts. Courts have grappled with the application of traditional policies, such as commercial general liability (CGL) to emerging cyber threats with mixed results for policyholders.

Pay Attention to Applicable Law

For example, in *St. Paul Fire & Marine Ins. Co. v. Rosen Millennium Inc.*, a hotel sent a demand letter to its data security provider (the insured) after discovering that hackers installed malware on the hotel's network and compromised customer credit card information.[1] The insured sought coverage under its CGL policy for the hotel's claim, but the court denied coverage. This case highlights the importance of framing a claim to the insurer with sufficient information to show it falls within coverage. Here, the court criticized the notice: "[t]he Notice of Claim is devoid of any substantive information other than the fact that a 'credit card systems breach occurred.'"

Rosen Millennium is also a reminder that both the jurisdiction and applicable law are critical. The policy defined "Personal Injury Offense" as "making known to any person ... covered material that violates a person's right of privacy." The court ruled that the insured could not satisfy this provision because the hackers published the information, not the insured. New York and Connecticut state courts have reached similar conclusions,[2] but federal courts in Virginia have found coverage under a CGL policy even though the policyholder did not publish the private information and even though there was no evidence that a third party ever viewed it.[3]

See "Don't Overlook Commercial General Liability Insurance to Defend a Data Breach" (Apr. 27, 2016).

Policy Wording Is Critical

Recent cases involving coverage under traditional crime policies for cybercrimes reinforce that the policy wording is critical for deciphering coverage (along with, as discussed above, jurisdictions and applicable law). Crime insurers have been aggressive in litigating cybercrime claims to try to avoid coverage by taking advantage of ambiguous or nuanced policy wording – oftentimes with success. For example, many crime insurers have sought to avoid coverage for social engineering claims by asserting that the fraudulent communication was not the "direct" cause of the loss because there was a supposed intervening event: the employee who mistakenly transferred the funds. Some courts have agreed.[4] In *Apache*, the insured received an email from fraudsters posing as a vendor directing the insureds to make payments to a new account. The court narrowly interpreted "direct" and upheld the coverage denial because the email was merely part of a scheme in which the employees played a role by changing the vendor's account information. Thus, the court concluded that "the email was merely incidental to the occurrence of the authorized transfer of money."

Policyholders Should Be Persistent

Recent U.S. Court of Appeals decisions may have stemmed the tide of unfavorable policyholder decisions.[5] For example, in *Medidata*, a fraudster "altered the emails that were sent to [company employees] to appear as if they were sent from [the insured's] president." Based on those fraudulent emails, the employee-initiated wire transfers to the fraudster's bank account. The insurer tried to deny coverage based on the argument that there was no "direct loss" as a result of the email spoofing attack because the employee intervened and processed the wire transfer. The court rejected that argument and found coverage. The court held that "direct" meant "proximate" and stated that "[t]he chain of events was initiated by the spoofed emails, and unfolded rapidly following their receipt. While it is true that the Medidata employees themselves had to take action to effectuate the transfer, we do not see their actions as sufficient to sever the causal relationship between the spoofing attack and the losses incurred."

Ultimately, in the event of a cybercrime, crime insurers' resistance to coverage claims should be met by policyholders' persistence in reinforcing the policy's language. Companies may be able to settle favorably, and they now have the benefit of favorable caselaw to combat coverage denials. However, given crime insurers' continual resistance to covering cybercrime claims, companies can best be served by obtaining cybercrime coverage through a cyber policy that is tailored to these types of risks.

See "Fixing the Chinks in Companies' Cyber Armor: Executives" (Feb. 20, 2019).

Obtaining the Right Policy

Obtaining a cyber insurance policy needs to be a thoughtful undertaking to ensure the policy can respond when the company needs it most and so the company is aware of any potential exclusions and limitations. A broker specializing (not dabbling) in cyber insurance and experienced insurance coverage counsel are critical resources that can help navigate companies during this process.

See "How Much Cyber Insurance to Buy Based on How Claims Are Paid" (Oct. 16, 2019).

Questions for the Cyber Insurer

Selecting the right cyber insurer is critical; not all cyber insurers are created equal. Some are experienced insuring cyber risks and are commercial during the underwriting and claims handling process; others are not. Key questions to ask when deciding on an insurer include:

- Does the insurer have a reputation for paying claims?
- Is the insurer experienced with cyber risks, or is the insurer new to the market?
- Is the insurer reasonable during the underwriting process?
- What are the policy's premiums, self-insured retention(s) and sublimits?

See "Dos and Don'ts of Choosing a Cyber Insurance Broker and Navigating the Application Process" (Jun. 12, 2019).

Do Your Diligence

During the underwriting process, pay careful attention to the policy application to prevent an insurer from later trying to rescind the policy or deny coverage because of a purported misrepresentation. Companies also must be prepared to answer questions about their company's financials, record count and claim history. Also, insurers will be keenly interested in vendor contracts – and whether and to what extent your company requires the vendor to provide indemnification or "additional insured" coverage. The insurer may also want to have an underwriting call to understand the company's network security. It will be critical to prepare the IT spokesperson to understand the purposes of the insurer's questions, focus on the question asked and avoid tangents.

Ask for More

Finally, cyber policies are dense, filled with numerous defined terms and exclusions, and ever-changing; the words of policies matter; and applicable law can be the difference between coverage or a denial. Coverage counsel can help companies understand the import of these words in a legal setting. Companies should not simply accept the wording initially proposed by the insurer. Policy terms often can be enhanced at the purchase or renewal stage – the company simply needs to ask. Therefore, companies should identify a "wish-list" of improvements to the policy form. While the company will probably not get the insurer to agree to every wish, it can likely secure some improvements that will carry through as the policy is renewed.

Eric Jesse is counsel in Lowenstein Sandler LLP's Insurance Recovery Group and Jason Meyers is an associate in that group. They have experience helping companies place and evaluate cyber insurance policies as well as assisting companies in handling cyber insurance claims following a cyber incident.

---

[1] 337 F. Supp. 3d 1176 (M.D. Fla. Sept. 28, 2018).

[2] *Zurich Am. Ins. Co. v. Sony Corp. of Am.*, 2014 WL 8382554 (N.Y. Sup. Feb. 21, 2014); *Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 15 A.3d 458 (Conn. 2015).

[3] *Travelers Indem. Co. of Am. v. Portal Healthcare Sols., LLC*, 35 F. Supp. 3d 765 (E.D. Va. 2014), aff'd 644 F. Appx. 245 (4th Cir. 2016).

[4] *Interactive Commc'ns Int'l, Inc. v. Great Am. Ins.*, 731 Fed. Appx. 929 (11th Cir. 2018); *Pestmaster Servs., Inc. v. Travelers Cas. Surety Co. of Am.*, 656 Fed. Appx. 332 (9th Cir. 2016); *Apache Corp. v. Great Am. Ins. Co.*, 662 Fed. Appx. 252 (5th Cir. 2016).

[5] *Am. Tooling Ctr., Inc. v. Travelers Cas. Surety Co. of Am.*, 895 F.3d 455 (6th Cir. July, 13, 2018); *Medidata Sol.s Inc. v. Fed. Ins. Co.*, 729 Fed. Appx. 117 (2d Cir. July 6, 2018).