The Legal Intelligencer
THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2020
PHILADELPHIA, TUESDAY, JULY 21, 2020 VOL 262 • NO. 14 An ALM Publication

CYBERSECURITY

Navigating Coverage for Losses, Liabilities Triggered by Cyber Attacks

BY ARTHUR R. ARMSTRONG
Special to the Legal

ARTHUR R. ARMSTRONG *is a shareholder in Anderson Kill's Philadelphia office and deputy co-chair of the firm's cyber insurance recovery group. Contact him at aarmstrong@andersonkill.com.*

> *"Purchasing the right insurance to cover cyber risk and pursuing a claim when a loss occurs are both complex tasks.*

Data security issues remain top of mind for c-suite executives, and for good reason. More and more data is being collected, tracked, retained and managed, while cyber-attacks against businesses—large and small—continue to increase in both frequency and sophistication. At the same time, significant data breach liability is being imposed through the European General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) and similar state statutes for organizations operating in those jurisdictions. EasyJet was recently the victim of a cyber attack that exposed personal data of nine million customers. The blowback was swift—plaintiffs attorneys commenced a class action lawsuit, quickly drawing over 10,000 plaintiffs from over 50 countries, making it almost instantly the largest data privacy suit in the U.K. Plaintiffs asserting claims under the GDPR need not even demonstrate any financial loss in order to be awarded damages. Mental distress is sufficient. If successful, the lawsuit against EasyJet could result in an $18 billion award.

In the face of this trifecta of risk—more companies possessing more data, increasing cyber attacks, and sky-high statutory liability—what is a business to do? Employing good cybersecurity practices, including robust breach-detection software, employee training and breach-response preparation, is a necessity. But these preventative measures are only half of the equation. No matter how strong a company's cyber program may be, a breach may occur. In this case, the ability to mitigate the loss by making a claim under the right insurance policy can be critical.

Purchasing the right insurance to cover cyber risk and pursuing a claim when a loss occurs are both complex tasks. Among the complicating factors: there is little uniformity in cyber policies, and different types of cyber policies cover different types of events; coverage can sometimes be found in traditional property, liability and crime policies; and the terms employed in filing a claim can be vital.

Cyber insurance is relatively young. Whereas property insurance policies have been around since the 1600s, providing many years of claims to evaluate for underwriting purposes, revisions to policy forms and judicial interpretations, cyber policies have a very short track record. Among other things, this means there is no "standard" cyber insurance policy or uniform interpretation of even the same policy language by courts. Each insurance company sells its own product, and the differences can be material.

Cyber insurance policies, even from the same insurance company, can come in different forms. Coverage may be through a stand-alone policy or a cyber endorsement to an existing policy. Coverage for loss caused by a cyber event may also be found in a policy that does not expressly reference a cyber attack at all—the so called "silent cyber" coverage.

In *National Ink & Stitch v. State Auto Property & Casualty Insurance,* 435 F. Supp. 3d 679 (D. Md. 2020) the court examined whether a property policy was triggered when the policyholder suffered a ransomware attack. State Auto argued that because the plaintiff only lost data, an intangible asset, and could still use its computer system to operate its business, it did not experience "direct physical loss" as required by the policy. National Ink countered that data and software were covered under the policy and that while the computer system still operated, impairment of functionality was enough to trigger the "direct physical loss" requirement. While courts are somewhat inconsistent on this issue, the *National Ink* court granted summary judgment to the plaintiff finding that loss of use, loss of reliability, or impaired functionality demonstrated the required damage to a computer system, consistent with the "physical loss or damage to" language in the policy. The court held that in many instances, a computer will suffer damage without becoming completely inoperable and that where a policyholder is left with a slower system, potentially harboring a dormant virus, the threshold for direct physical loss has been met.

As coverage for a loss caused by a cyber attack may be found in various policies, early evaluation is key. There is a minefield of potentially costly errors in overlooking coverage or invoking the wrong policy provision. For example, defined terms may sound similar at first blush, but reference to the wrong one could make it more likely the claim will be denied, or possibly implicate a sublimit that is far too low to cover the actual loss. Defined terms like "privacy event," "security failure," "network interruption" and the like must all be carefully scrutinized and the interrelationship understood in order to properly frame a cyber insurance claim.

Facts like whether the identity of the threat actor has been determined can also have significant effects on which coverage grant is triggered—a loss caused by a disgruntled employee may have a different limit than a cyber attack from a third party. Likewise, not all cyber attacks involve an actual technical breach of an organization's cyber security defenses. A phishing attack, where a threat actor convinces an employee to undertake some action such as wiring money or providing password information, can result in a significant loss even where the cyber defenses were not technically breached. Likewise, a DDoS attack—an attempt to overwhelm a website with internet traffic—can bring a webpage down without actually infiltrating the network. But the damage it causes is just as real.

Importantly, not all cyber policies cover the same types of events. Some may provide coverage for defending against third party actions, like the EasyJet class action, whereas others provide coverage for first party losses, such as unintentionally wiring a payment from a corporate account as a result of a phishing attack. Many policies provide both. But good guidance from a knowledgeable insurance broker is key to ensure that all risks a company may face are appropriately addressed. Likewise, involving coverage counsel early will help avoid any missteps that open the door for the insurance company to mischaracterize a loss under a low sublimit or deny outright when coverage actually exists.

After a cyber attack has been identified, stopping the attack, restoring data and fixing any vulnerabilities are top priorities. But to mitigate the financial loss, a policyholder should be sure to timely analyze its rights under all available insurance that could respond. This may be under a stand-alone cyber policy or endorsement, or could be under a property, crime, or other policy that could cover the loss. Remember, an insurer may appoint its designated breach response team after being notified of a cyber attack, but this team will not include an attorney to advise the policyholder on insurance coverage, an issue that will play out after the cyber attack itself has been controlled. But rest assured the insurance company has its counsel evaluating whether coverage for any part of the loss may be excluded or otherwise denied. The policyholder is well served to consult knowledgeable coverage counsel as well to ensure all reasonable avenues to coverage are pursued. ●