September 10, 2021
ARTICLES

Cyberattacks—A Spotlight on Ransom Losses and Insurance

An overview of insurance coverage for cyber losses and court decisions that address the various ways in which cyberattacks have been analyzed for coverage by the courts.

By Pamela D. Hans

Where Are We and How Did We Get Here?

According to the annual Internet Crime Reports by the Federal Bureau of Investigation (FBI), cybercrime losses rose more than sixfold from 2009 ($560 million) to 2019 ($3.5 billion). [1] The year-over-year trend just between 2018 and 2019 shows almost a $1 billion increase in the reported losses and an increase of more than 30 percent in reported events. [2]

Not only has the number of cybercrimes increased—so has the sophistication and severity of the crimes. The recent Solar Winds attack that targeted agencies within the U.S. federal government—including the Departments of Homeland Security, Energy, Commerce, Treasury, and State—shines a bright light on how dangerous, pervasive, and sophisticated cybercriminals have become. [3]

According to the FBI, the most frequently reported complaints in 2019 were phishing and similar ploys, nonpayment/non-delivery scams, and extortion. The most financially costly complaints involved business email compromise, romance or confidence fraud, and spoofing.

Against this backdrop of escalating risk, we turn to a discussion of the insurance coverage that may be available to businesses and a discussion of the analysis that courts have used to determine whether a cybercrime is covered by insurance.

Where Businesses Can Look for Coverage When Experiencing a Cybercrime Loss

The first question for any business that experiences a cyberattack may not always be related to insurance. However, whether or not insurance covers a business's losses should be one of the first questions to ask.

As a starting point, consider the various aspects of a data breach or other cybercrime and the losses that result. Cybercrimes typically require an investigation into the incident and reporting of the incident to law enforcement and to the individuals whose data were compromised. Decryption of the data, restoration of the system, and hardening of the system to ensure that the threat actor is no longer present or able to redeploy malware from inside the network are also expenses that result from a breach. Those steps, along with implementing the necessary repairs, can result in business interruption losses—both to the target of the cyberattack and also those businesses that rely on that target for data storage, network support, or other support.

Many of these losses may be covered by insurance. A close review of a business's insurance policies—all of them, not just cyber-specific policies—is essential to maximizing the recovery.

For many companies, one or more insurance policies within their insurance program may cover several aspects of ransomware and other cyberattacks. Data breaches can cause harm to the company's network (i.e., company property) as well as someone else's property or business. Consider, for example, a cyberattack that paralyzes a network that a company operates but that others rely on. The attack may cause loss to the company's network, damage the data and equipment that belong to third parties, and cause business interruption losses to those third parties. This situation implicates both first-party insurance that covers losses to the company's own property and third-party liability coverage. Because breaches often involve a hacker's access to and theft of information stored in computer networks, it is not uncommon to see third-party liability claims arising out of a data breach. Looking only to first-party policies, or even cyber-specific policies alone, may unduly limit the universe of insurance coverage and policies that may respond to data breach losses.

Coverage for cyber-related losses is generally found in two segments of the coverage spectrum. The first may be the most obvious—a cyber insurance policy, whether basic or tailored. Basic cyber insurance policies typically cover losses such as event management, data privacy breaches, network security liability, privacy regulation investigation, cyber extortion, and restoration of data and cyber assets. A tailored cyber policy may cover the losses enumerated above and also business interruption losses, regulatory investigation, and dependent network interruption.

At the other end of the spectrum is so-called "silent" cyber coverage inherent in policies that are not cyber-specific. These include third-party liability policies (e.g., commercial general liability policies), property policies, directors' and officers' (D&O) and errors and omissions (E&O) policies, and crime policies.

There are two types of so-called "silent" cyber coverage: one type in which the insurance company truly did not intend to underwrite cyber risks in the policy, and the other in which claims have some nexus with cyber and clearly fall within the type of coverage at issue. In the first category, a D&O policy may provide coverage for securities suits that allege negligence that harms the company's stock price. In the second category, kidnap and ransom coverage, or specialty crime coverage, may respond to some cyberattacks, such as ransomware attacks for the former or phishing attacks for the latter.

When notifying insurance companies of a cyber loss, it is prudent not to overlook the possibility that the company's non-cyber policies may provide silent cyber coverage for specific types of loss. While an insurance company may at first deny coverage for a cyber loss submitted under a non-cyber policy, the details of the policy matter and the denial may not stand. As the cyber market evolves, insurance companies are slowly trying to eliminate "silent cyber" in favor of tailored—and expensive—cyber coverage.

If they haven't yet managed to incorporate an exclusion that eliminates silent cyber, however, their wish that the coverage does not exist does not make it so. Policyholders should take time to closely analyze their insurance policies and, where warranted, challenge their insurance companies' coverage positions.

Common Insurance Coverage Issues

As data breach and other cybercrime coverage disputes make their way through the courts, decisions to date highlight that policyholders should not necessarily accept coverage denials; where warranted, they should challenge denials of coverage as well as insurance company characterizations of the loss.

In one recent case in which a court found coverage for a cyberattack, *National Ink & Stitch LLC v. State Auto Property & Casualty Insurance Co.*, the issue was coverage under a first-party property policy for the replacement cost of servers damaged by a ransomware attack.[4] The hacker perpetrated a ransomware attack on a U.S. business, National Ink & Stitch, locking the business out of its own computer system. In

exchange for Bitcoin, the hacker agreed to release the computer system back to the control of the owner. After Ink & Stitch paid the ransom, the hacker eventually restored modest control of the computer system, but issues remained. Ink & Stitch still could not access all its files, the computer system ran much more slowly, and tech experts confirmed that dormant remnants of ransomware virus could reinfect the entire system at any time. The only solution was to wipe the system or get a brand new one. The insurance company denied coverage asserting that there was no direct physical loss, and thus no damage, and no covered loss.

Ink & Stitch filed a claim under a businessowner's policy with a computer coverage endorsement that expressly covered damage to electronic media and records and data stored on such media. Nonetheless, the insurance company, State Auto Property and Casualty Insurance, denied coverage, arguing that the damage to Ink & Stitch's computer system—the lost files, the slower processing speeds, and the dormant virus that could disable the computer system at any time—were not "direct physical loss of or damage to" the computer system under the insurance company's standard "businessowner's insurance policy."

The court disagreed, finding that "the more persuasive cases are those suggesting that loss of use, loss of reliability, or impaired functionality demonstrate the required damage to a computer system" to trigger this type of policy, requiring the insurance company to cover such losses and damage.

This case illustrates not only that cyber coverage may be sold under a variety of policy types but also that the purchase of policies that expressly cover the salient risks does not guarantee coverage. Further, policyholders should not take a coverage denial at face value without close analysis of the policy language. They should not assume that only ransom is covered, and they should look for coverage under all available policies.

Is a Cyberattack Computer Fraud?

One common means by which cybercriminals have been stealing from businesses is through email spoofing or other social engineering in which the threat actor uses a forged email address. The objective in these attacks is to make the recipient think the email is from someone the recipient knows. In many such cases, the recipient is tricked into sending a wire transfer of funds to the fraudster. The agency of the tricked employee raises coverage issues under various policy types.

In *Medidata Solutions, Inc. v. Federal Insurance Co.*, the policyholder was targeted by a threat actor who directed an employee to process a wire transfer.[5] In an email, the threat actor posed as Medidata's president using a forged email address. The threat actor sent emails and placed phone calls to employees, who followed the wire transfer instructions received from the threat actor and transferred $4.8 million to the fraudsters.

Medidata filed a claim under its insurance policy with Federal Insurance Company. The Federal insurance policy contained a crime coverage section that covered loss caused by forgery, computer fraud, and funds transfer fraud.[6] Federal nonetheless denied coverage, claiming there was no coverage under the computer fraud provision because there was not a "fraudulent entry of Data into Medidata's computer system." Federal also denied coverage under the funds transfer fraud clause because the wire transfer was authorized by Medidata employees. Federal denied forgery coverage, asserting that the emails did not contain a signature and did not meet the policy's definition of a financial instrument.

Under Medidata's policy, a computer violation occurs upon (a) a fraudulent entry of data into or deletion of data from a computer system or (b) a fraudulent change to data elements or program logic of a computer system, which is kept in machine-readable format.

Medidata argued that Federal's denial was incorrect because the theft was covered by the policy's funds transfer clause. According to Medidata, the loss was covered because the theft (1) caused a direct loss of money (2) by fraudulent electronic instructions purportedly issued by Medidata (3) issued to a financial institution (4) to deliver money from Medidata's accounts (5) without Medidata's knowledge or consent.[7]

The court concluded that Medidata demonstrated that the funds transfer fraud clause covered the theft in 2014.

> The Policy defines Funds Transfer Fraud as: "fraudulent electronic . . . instructions . . . purportedly issued by an Organization, and issued to a financial institution directing such institution to transfer, pay or deliver Money or Securities from any account maintained by such Organization at such institution, without such Organization's knowledge or consent.[8]

The court reasoned that because a third party disguised itself as an authorized representative and directed Medidata's accounts payable employee to initiate the electronic bank transfer, even though the employee "willingly pressed the send button on the bank transfer," the accounts payable personnel would not have initiated the wire transfer but for the third party's manipulation of the emails. In short, the fact that an employee initiated the transfer does not transform the bank wire into a valid transaction. Because the wire transfer was dependent on consent that was obtained by trickery, the court concluded that Medidata had demonstrated that the funds transfer fraud clause covered the theft in 2014.

For the court in *Medidata*, the dispute turned on whether the spoofing emails that set the theft in motion constituted "the fraudulent entry of data" under the Federal policy. According to Federal, those emails did not "cause any fraudulent change to data elements or program logic of Medidata's computer system" and there was "no direct nexus" between the spoofing email and the loss because Medidata employees took intervening and independent steps that resulted in the initiation of the wire transfer. The court, however, took a different view. Focusing instead on the steps that the hacker took to disguise the true origin of the

email address, the court found that there was a "fraudulent entry of data into the computer system" and "a change to a data element" when the hacker used computer code to disguise the true origins of the spoofed email.[9]

Other courts faced with a similar question have taken a different route to reach the same result. In *American Tooling Center, Inc. v. Travelers Casualty & Surety Co. of America*, the plaintiff policyholder was targeted by hackers who were disguised as one of its vendors.[10] As in *Medidata*, the policyholder's employees initiated a wire transfer to the imposter. When American Tooling Center submitted a claim to Travelers under the "Computer Fraud" portion of its insurance policy, Travelers denied coverage. According to Travelers, the policy required that a computer "fraudulently cause the transfer."[11] Travelers asserted that because a person—not a computer—knowingly initiated and caused the transfer, there was no computer fraud as defined in the policy. The Sixth Circuit, however, rejected Travelers' arguments. The court focused on what ultimately set the wire transfer approval process in motion and concluded that the fraudulent email was that catalyst. Thus, the court concluded that the transfer was directly caused by computer fraud as defined by Travelers' policy.

Noteworthy in *Medidata* and *American Tooling Center* is that although the courts reached the same conclusion, that the losses were covered by the insurance policy, they followed different logical trails to get there. In *American Tooling Center*, the court looked to the fact that the transfer was "induced by a fraudulent email" and thus caused by computer fraud. In *Medidata*, however, the court evaluated the spoofed emails as involving a "fraudulent entry of data into the computer system" because the true source of those emails was masked by computer code. That change to a "data element," as the court said, occurred when the hacker used computer code to mask the spoofed email's true origins. The court further reasoned that the losses "were directly caused by the computer fraud" because the chain of events that resulted in the $4.8 million wire transfer was initiated by the spoofed emails. The *Medidata* court focused on fraudulent intent, whereas the *American Tooling Center* court focused on the physical fact that the fraudsters entered data into the target's computer system.

In *Cincinnati Insurance Co. v. Norfolk Truck Center*, as in *American Tooling Center*, the court concluded that a policyholder's loss was covered by the computer fraud coverage part of its insurance policy that covered "loss of . . . money . . . resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside" the policyholder's offices.[12] According to Cincinnati Insurance, the policy did not cover the loss because the loss did not result directly from the use of a computer, a legitimate invoice caused the wire transfer (as opposed to an email), and the intervening individuals involved who issued the wire transfer broke the chain of events such that the loss did not result "directly from the use of any computer to fraudulently cause a transfer. . . ."

The court rejected the insurance company's approach. In determining that the loss was covered, the court looked at the entire chain of events that preceded the wire transfer and observed that computers were

involved in each step of the process. The court noted that the cause of the transfer must be fraudulent—not necessarily the payment itself. Accordingly, even though the payment was for a valid invoice, the instructions were fraudulent, initiated by an email and the use of a computer. Thus, the court concluded that the loss was covered by the policy because that loss resulted directly from the use of a computer, notwithstanding the various intervening steps that did not involve a computer.

An Eleventh Circuit decision rejected yet another insurance company's parsing of a policy provision purporting to cover fraud—in this case, a provision expressly designed to cover wire transfer induced by fraudulent instruction. In *Principle Solutions Group, LLC v. Ironshore Indemnity, Inc.*, the insurance policy covered "loss resulting directly from a fraudulent instruction directing a financial institution to debit the insured's transfer account, and transfer, pay or deliver money or securities from that account."[13] The policy defined "fraudulent instruction" as "an electronic or written instruction initially received by the insured, which instruction purports to have been issued by an employee but which in fact was fraudulently issued by someone else without the insured's or the employee's knowledge or consent."[14] The scenario in *Principle Solutions* is much the same as in *American Tooling Center* and *Norfolk Truck Center*; that is, a hacker disguised its email address to induce another to initiate a wire transfer. In *Principle Solutions*, however, the insurance company denied coverage on the basis that the fraudulent email did not instruct an employee to wire a specific sum of money. The insurance company further argued that another email involved in the scheme, from a fake lawyer to a bank providing wire transfer instructions, did not fall within the scope of a fraudulent instruction because the email was not from an employee of the policyholder. The court, rejecting the insurance company's arguments, reasoned that the emails, taken together, were part of the same fraudulent instruction and the resulting loss was covered by the fraudulent instruction coverage in the policy.

A comparison of these four cases highlights the importance of nuances in policy language in an analysis of insurance coverage for cyber losses. In each of the cases, the policyholder suffered a loss because an employee trusted information in an email sent by a hacker. While each court concluded that the loss in question was covered as computer fraud as defined by the particular insurance policy, each court used a slightly different analytical approach and considered different policy language to reach the same conclusion. Policyholders should take heart that courts, including three federal appeals courts, are rejecting insurance companies' tortured assertions that losses clearly induced by fraud as defined in their policies are not in fact induced by fraud. While successful challenges to such coverage denials require a close reading of the policy language, careful analysis of the facts, and a precise reading and application of the law, a clear sense of the intent of the fraudster and the intent of the policy should encourage policyholders to persist in these cases.

Pamela D. Hans is the managing shareholder of Anderson Kill P.C.'s Philadelphia office.

[1] Fed. Bureau of Investigation, Internet Crime Complaint Ctr., *2009 Internet Crime Report* (2010); *2019 Internet Crime Report* (not dated).

[2] Fed. Bureau of Investigation, IC3 Complaint Statistics 2014–2018.

[3] Kari Paul & Lois Beckett, "What we know—and still don't—about the worst-ever US government cyber-attack," *Guardian*, Dec. 19, 2020.

[4] *Nat'l Ink & Stitch LLC v. State Auto Prop. & Cas. Ins. Co.*, No. SAG-18-2138 (D. Md. Jan. 23, 2020).

[5] *Medidata Sols., Inc. v. Fed. Ins. Co.*, 729 F. App'x 117 (2d Cir. 2018).

[6] *Medidata Solutions*, 729 F. App'x 117.

[7] *Medidata Solutions*, 729 F. App'x 117.

[8] *Medidata Solutions*, 729 F. App'x at 480.

[9] *Medidata Solutions*, 729 F. App'x 117.

[10] *Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am.*, 895 F.3d 455 (6th Cir. 2018).

[11] *American Tooling Center*, 895 F.3d 455.

[12] *Cincinnati Ins. Co. v. Norfolk Truck Ctr.*, 430 F. Supp. 3d 116 (E.D. Va. 2019).

[13] *Principle Sols. Grp., LLC v. Ironshore Indem., Inc.*, 944 F.3d 886 (11th Cir. 2019).

[14] *Principle Solutions Group*, 944 F.3d 886.

Endnotes