NEW JERSEY LAWYER

October 2021

No. 332

INSURANCE

A Hack a Day—Can Insurance Keep the Resulting Losses Away?

How Insurance Protects Against Cyber Risks and How Courts Interpret Coverage

by Kimberly Parson and Eugene Killian

The 1996 movie *Independence Day*, like many books and movies that are more than a few years old, now seems hilariously dated with respect to technology. As you probably know, the movie involves the invasion of earth by massive, murderous alien spaceships. At one point, David Levinson (Jeff Goldblum), the movie's computer nerd, is sitting on the floor contemplating the fate of humanity. Julius Levinson (Judd Hirsch), his father, tells him to get up before he catches a cold. That creates the light bulb moment in David's mind. He'll give the alien computers a "cold!" A "virus!" That will save the day!

Difficult as it is to believe 25 years later, a computer virus was a novel and mystifying concept to most moviegoers in 1996.

This past Independence Day weekend, things became more real, with one of the largest criminal ransomware attacks ever. Kaseya, a global IT infrastructure provider, suffered an attack that utilized its Virtual System Administrator (VSA) software to deliver REvil (also known as Sodinokibi) ransomware to customers through an automatic update. Between 800 and 1,500 small businesses and other organizations had their data encrypted, including a grocery store chain and several schools. Eventually and fortunately, Kaseya was able to obtain a decryption key from an unidentified third party. Sadly, these types of attacks are expected to continue indefinitely, in part because the Russian government will do nothing to stop them as long as they do not target Russian interests.

The Kaseya attack, and other recent high-visibility attacks such as the one on Colonial Pipeline, have again made the issue of insurance coverage for cyber-losses a hot topic. To what extent does insurance protect against, among other things, liability for costs incurred by customers and other third parties, the cost of repairing or replacing lost systems and data, losses from business closure or slowdowns, regulatory fines for failure to adhere to state and federal-mandated compliance requirements for protecting cus-

tomers' data, and related lawsuits? The answers remain largely unclear, with Courts continuing to render seemingly contradictory rulings.

Businesses continue to look to various types of insurance policies to protect from losses and liabilities arising from cyber-attacks and IT-related incidents. These include what the insurance industry has labelled "silent cyber" coverage, such as the following:

- **Comprehensive General Liability** (CGL) policies for property damage (to tangible property), as well as personal and advertising injury liability coverage for injuries caused by the publication of material that violates a right to privacy.
- **Crime Insurance** coverage, which protects against loss of property resulting from intrusion into a computer system, and typically insures against the "direct loss of, or direct loss from damage to," money, securities and other property "directly" caused by fraud.

Unfortunately, policyholders seeking to enforce coverage under CGL or crime insurance coverage are often in for a fight. Given the high level of exposure for cyber-liability, insurance companies tend to construe these policies very narrowly, and often argue that coverage for most hacking incidents was never intended.

Stand-alone cyber coverage is also available, although underwriting requirements for such policies are now tightening due to the proliferation of attacks. Broadly speaking, cyber insurance policies specifically cover the costs of cybersecurity failures, including data recovery, system forensics, and the costs of defending lawsuits and making reparations to customers. There is no standard form of cyber policy, and little decisional law interpreting coverage.

Cyber coverage cases under "traditional" business policies generally fall into four categories. First, cases under CGL or property policies finding that coverage exists due to a user's computer hardware being rendered inoperable. In these cases, Courts find that the requirement of tangible "property damage" has been met.[1] Second, and conversely, cases finding no coverage where only data was lost, on the theory that data constitutes uncovered "intangible" property.[2] Third, cases involving the "personal injury" coverage in a CGL policy, sometimes turning on whether there has been a required "publication" of private information.[3] Fourth, cases finding no coverage where the policyholder's system was breached by a third party who accessed customer information, but the alleged "publication" was by the third party and not by the policyholder. The theory of noncoverage for this type of claim is that the policy only provides coverage for the policyholder's acts or omissions, and not those of third parties.[4]

As a recent example of a claim for cyber liability coverage under a CGL policy, *Landry's, Inc. v. The Insurance Co. of the State of Pennsylvania*[5] involved a policyholder (Landry's) that operates retail properties including restaurants, hotels, and casinos. Landry's discovered a data breach that occurred between May 2014 and December 2015, involving the unauthorized installation of a program on its payment processing devices. For over a year, the program retrieved personal information from millions of credit cards, and at least some of that information was used to make unauthorized charges. The losses totaled over $20 million.

KIMBERLY M. PARSON *is the managing partner of the New Jersey office of Rebar Kelly. She has over 15 years of experience representing clients in insurance coverage litigation and providing coverage opinions and advice to insurance carriers concerning their coverage obligations under various types of insurance policies.*

EUGENE KILLIAN, JR. *is the principal member of The Killian Firm, P.C., and has been handling insurance coverage matters for policyholders for 37 years.*

Unfortunately, policyholders seeking to enforce coverage under CGL or crime insurance coverage are often in for a fight. Given the high level of exposure for cyber-liability, insurance companies tend to construe these policies very narrowly, and often argue that coverage for most hacking incidents was never intended.

Landry's credit card processing company, Paymentech, faced large claims from Visa and MasterCard as a result of the breach, and sued Landry's, contending that the losses resulted from Landry's not following proper security procedures.

Landry's filed a claim with its insurance company, ICSOP, requesting a defense to the Paymentech lawsuit. The "personal injury" part of the ICSOP policy covered liability for damages "arising out of the oral or written publication of material that violates a person's right of privacy."

The Court first held that the requisite "publication" had been alleged, writing:

> The *Paymentech* complaint plainly alleges that Landry's published its customers' credit-card information-that is, exposed it to view. In fact, the *Paymentech* complaint alleges two different types of "publication." The complaint first alleges that Landry's published customers' credit-card data to hackers. Specifically, as the credit-card "data was being routed through affected systems," Landry's allegedly exposed that data-including each "cardholder name, card number, expiration date and internal verification code." Second, the *Paymentech* complaint alleges that hackers published the credit-card data by using it to make fraudulent purchases. Both disclosures "expos[ed] or present[ed] [the credit-card information] to view."

Next, the Court, using an apt food analogy, found that the requisite invasion of privacy had also been alleged, writing:

> ICSOP urges us not to follow the plain text of the Policy and instead to alter it. In ICSOP's view, the Policy covers only *tort* damages "arising out of...the violation of a person's right of privacy." Thus, ICSOP suggests, it might defend Landry's if it were sued *in tort* by the individual customers who had their credit-card data hacked and fraudulently used. But ICSOP thinks it bears no obligation to defend Landry's in a *breach-of-contract* action brought by Paymentech. Of course, the Policy contains none of these salami-slicing distinctions.

Other policyholders have looked to their crime coverage for computer fraud issues. With respect to crime coverage, several Courts have found that no required "direct loss" has occurred where unwitting personnel transferred funds as the result of fraudulent communications via computer by imposters.[6] Other Courts have disagreed, finding that the policyholder suffered a "direct loss" because the fraudulent communication entered the policyholder's computer system, and computers were involved in the resulting loss.[7]

A recent interesting decision, *G&G Oil Co. of Ind., Inc. v. Cont'l W. Ins. Co.*,[8] involved the question of insurance coverage under a crime policy for a ransomware attack. After having its data locked by criminals. G&G Oil negotiated the decryption of its data in exchange for a ransom payment. G&G Oil then turned to its insurance company, Continental, which had sold a policy including coverage for, among other things, losses "resulting directly from the use of any computer to fraudulently cause a transfer of…property." Continental denied coverage, in part because G&G Oil had voluntarily paid the hacker. According to Continental, its policy only covered losses where the hackers themselves transferred the funds.

The Indiana Supreme Court first held that the term "fraudulently cause a transfer" can be reasonably understood as simply "to obtain by trick." According to the Court, a trial was needed to determine whether the hackers had accessed G&G Oil's systems through trickery, or whether the hackers simply entered the system unhindered.

With respect to whether the ransomware attack "directly" caused G&G Oil's loss, the Court held that this provision meant that G&G was required to show that its loss resulted either "immediately or proximately without significant deviation from the use of a computer." The Court held that this requirement was satisfied, writing:

> Analyzing G&G Oil's actions in this case, its transfer of Bitcoin was nearly the immediate result—without significant deviation—from the use of a computer. Though certainly G&G Oil's transfer was voluntary, it was made only after consulting with the FBI and other computer tech services. The designated evidence indicates G&G Oil's operations were shut down, and without access to its computer files, it is reasonable to assume G&G Oil would have incurred even greater loss to its business and profitability. These payments were "voluntary" only in the sense G&G Oil consciously made the payment. To us, however, the payment more closely resembled one made under duress. Under those circumstances, the "voluntary" payment was not so remote that it broke the causal chain. Therefore, we find that G&G Oil's losses "resulted directly from the use of a computer."

The bottom line is this. Cyber losses are never going away, because, to paraphrase famed bank robber Willie Sutton in another context, "That's where the money is." Enforcing coverage for such losses under general business policies will continue to be difficult, because insurance companies do not want to create precedent by freely paying claims in an area involving such huge exposure. Preventing losses through training and vigilance is the best protection for businesses. If losses happen, stand-alone cyber insurance policies are far more likely to provide necessary coverage for a variety of first-party and third-party losses. Because we face an environment

of exponentially increasing cyber attacks, principally through ransomware, premiums for specific cyber coverage are increasing, and underwriting requirements are more stringent. Policyholders who obtain such coverage can expect to see increased deductibles and more sub-limits, such as for ransomware attacks.[9] ⚖

Endnotes

1. *Eyeblaster, Inc. v. Federal Insurance Co.*, 613 F.3d 797, 800-02 (8th Cir. 2010) (Minnesota law) (claim covered where visit to insured's website caused damage to third-party's computer, i.e., tangible property, rendering it inoperable, due to infection with spyware and other malicious programming from the insured's website); and *Retail Systems, Inc. v. CNA Ins. Companies*, 469 N.W. 2d 735, 738 (Minn. App. 1991) (Third-party liability policy covering "physical injury or destruction of tangible property" was held to cover damages for the loss of computer tape containing results of a voter survey; the computer tape and associated data were tangible property as defined in the policy).
2. *Ward General Ins. Servs., Inc. v. Employers Fire Ins. Co.*, 114 Cal. App. 4th 548, 7 Cal. Rptr. 3d 844 (2003), *as modified on denial of reh'g* (Jan. 7, 2004) (Insured filed action against insurer for declaration that its commercial policy covered losses incurred when data in its computer was inadvertently deleted, but Court held that data alone constitutes intangible property; thus, no coverage); and *Ciber, Inc. v. Federal Insurance Company*, Case No. 16-cv-01957-PAB-MEH, 2018 WL 1203157 (D. Colo. Mar. 3, 2018) (where customer alleged that software designed by insured failed to perform as required; this did not constitute damage to tangible property, as this involved shortcomings in the insured's software product, which is intangible property).
3. *Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 317 Conn. 46, 50-51, 115 A.3d 458 (2015) (after tapes containing personal information of employees fell off truck and was retrieved by unknown individual, Court ruled this did not constitute a "personal injury" as defined by the policies because there had been no "publication" of information stored on the tapes resulting in a violation of a person's right to privacy, because there was no proof the lost information had been accessed, i.e. published to a third party); but see *Travelers Indem. Co. of Am. v. Portal Healthcare Sols., L.L.C.*, 644 F. App'x 245, 248 (4th Cir. 2016) (Virginia law) (hospital contracted with the insured for electronic storage of confidential medical files, a class action was filed after a patient's Google search for her name resulted in links that allowed direct access to patient's medical records; insurer had duty to defend, because allowing confidential medical records to be publicly accessible via the internet constitutes "publication" of those materials resulting in personal injury; and stated that publication occurs when information is "placed before the public," not when a member of the public reads the information place before them, so the medical records were published the moment they became accessible to the public).
4. *Zurich Am. Ins. v. Sony Corp. of Am.*, No. 651982/2011, 2014 WL 8382554, 2014 N.Y. Misc. LEXIS 5141 (N.Y. Sup. Ct. Feb. 21, 2014) (after confidential information was released following an illegal intrusion into Sony's secured sites, Court ruled, from the bench on motions, that there was no coverage for the hacking and related release of information, because publication by a third-party does not trigger coverage under CGL policy; as the policy provided coverage for "acts or omissions of an insured that causes covered losses to a third-party" not acts and omissions of third-parties that cause damage to the insured or others); *St. Paul Fire & Marine Ins. Co. v. Rosen Millennium, Inc.*, 337 F. Supp. 3d 1176, 1185-86 (M.D. Fla. 2018) (following a credit card breach caused by malware installed in insured's payment network, court denied coverage on the basis that