CARTER/LEDYARD

our resources

Cyber Risk and Insurance: Limited Protection from Traditional Commercial General Liability Insurance

March 06, 2018

Client Advisory

March 6, 2018 by Mark R. Zancolli, H. Thomas Davis, Jr., John M. Griem, Jr. and Matthew B. James

This is the first of four Client Advisories concerning cyber risk and insurance. This Advisory discusses the limited protection which traditional commercial general liability ("CGL") insurance provides for losses from cybersecurity incidents. Subsequent Advisories will discuss the limitations of commercial crime insurance, the limitations of some cyber insurance policies, and items to consider when purchasing cyber insurance policies.

The theme of these Advisories is that a business that relies solely on traditional insurance such as a CGL policy to cover cyber risks is likely in for an unpleasant surprise, and that language in a cyber insurance policy can provide its own unfavorable surprises unless thoughtfully reviewed, negotiated and drafted.

The extent of cyber risk. In light of the rapidly advancing sophistication and frequency of data breaches, denial of service attacks, social engineering fraud (such as email spoofing scams) and other cybersecurity events, businesses must immediately consider addressing their cyber risks through insurance as part of their cybersecurity risk management strategy. No person or entity is immune from cyber risk. This fact is evidenced by, among other attacks, the "WannaCry" ransomware attack last May (encrypting the data on an estimated 300,000 victims' computers in over 150 countries and demanding "ransom" in Bitcoin for decryption) [1] and the data breach experienced by Equifax last May to July (involving unauthorized access to the personal data of approximately 148 million U.S. consumers – including names along with Social Security numbers, credit card numbers and/or driver's license numbers). [2]

The costs associated with a cyber event are often devastating. A recent study found that, for a U.S. company, the average organizational cost of a single data breach involving fewer than 100,000 records was $7.35 million in FY 2017.[3] Of course, several data breaches have resulted in costs and compromised record totals far exceeding those figures (as described in our April 2017 advisory). Additionally, it has been predicted that global ransomware damage costs will rise to $11.5 billion in 2019 (up from $325 million in 2015) and that damage costs from cybercrime will reach $6 trillion annually by 2021. [4]

Given the heightened risk and formidable cost of a cyber event, the value proposition presented by insurance coverage that transfers financial risks associated with a cyber event to an insurance company is very compelling. That being said, coverage for many types of cyber-related losses under traditional insurance policies such as CGL policies has become increasingly uncertain due to, among other things, the varied outcomes of court cases involving coverage disputes for cyber-related losses under traditional policies, as well as endorsements that have been added by some insurers to traditional policies to exclude coverage for cyber risks. As a result, in recent years, there has been growing demand for – and more insurers have offered – cyber insurance policies to cover an insured's direct costs and liability to third-parties resulting from a cyber event. Unlike traditional policies, cyber policies lack standardized language and have not been the subject of many court decisions thus far due to their relatively recent vintage. Businesses must carefully review the wording of their existing insurance policies with legal counsel and

an insurance broker to ensure that the policy language would meet their business needs in the event of a cyber event, and to explore what additional coverage options are available to address any existing gaps in coverage.

Insurable Losses. The costs that a company experiencing a cyber event may incur include "first-party" losses, which are direct losses and out-of-pocket expenses the company incurs, and "third- party" losses, which are liabilities and expenses the company incurs as a result of claims against it. First-party losses from a cyber event may include such items as forensic investigation costs, customer notification expenses, business interruption losses, loss or damage to digital assets, theft of money, cyber extortion losses, and public relations expenses. Third-party losses from a cyber event may include litigation defense costs, settlements, judgments, regulatory defense costs, fines and penalties.

Commercial General Liability Insurance. Most businesses have a CGL insurance policy. CGL policies typically include provisions covering liability for "**bodily injury and property damage**" and "**personal and advertising injury**." While many people may think of CGL policies within the context of providing coverage for slip and fall accidents and other types of premises liability, some policyholders have made successful claims for coverage of losses resulting from a cyber event under CGL policies, although the ability to do so has become highly doubtful with respect to many types of cyber risks. Court decisions involving disputes for coverage under CGL policies with respect to cyber events have largely focused on whether the policyholder's claim for coverage under the policy either fell within the policy's definition of "property damage" or under the policy's definition of "personal and advertising injury."

"Property damage" is typically defined in CGL policies as "physical injury to tangible property, including all resulting loss of use of that property" or "loss of use of tangible property that is not physically injured," and CGL policies typically provide that tangible property does not include electronic data. Some courts have found coverage under a CGL policy's definition of "property damage" for claims against an insured with respect to damage to, or a loss of use of, tangible property (such as a computer) as a result of a cyber event. For example, in the case of *Eyeblaster, Inc. v. Federal Ins. Co.*, the insured sought a declaratory judgment that its insurer had a duty to defend it in a lawsuit brought by a person who alleged that his computer was infected by a spyware program when he visited a website owned and operated by the insured, which allegedly caused his computer to freeze up and lose certain data. 613 F.3d 797, 800 (8th Cir. 2010). The Court of Appeals for the Eighth Circuit ruled that the claims in the lawsuit against the insured were covered under the insured's general liability policy, since the complaint against the insured alleged a "loss of use" of a computer and therefore fell within the policy's definition of covered "property damage" as "loss of use of tangible property that is not physically injured." In doing so, the court reversed the lower court's ruling in favor of the insurer that there was no coverage because the complaint against the insured alleged damage to software and the policy's coverage for "property damage" excluded "any software, data or other information that is in electronic form." *Id.* at 801-802.

However, most courts have found that claims arising from a loss of electronic data, such as payment card information, do not come within a general liability policy's coverage for "property damage." For instance, in the case of *RSVT Holdings, LLC v. Main Street America Assurance Co.*, 136 A.D.3d 1196 (N.Y. App. Div. 3rd Dept. 2016), the insureds, operators of fast food restaurants, suffered a data breach in which their network was infiltrated by unknown persons who unlawfully obtained customer credit card information and used it to make fraudulent charges. The insureds were subsequently sued by a bank alleging that it was required to reimburse fraudulent charges made to its credit cardholders' accounts as a result of the insureds' negligence in failing to safeguard the cardholders' credit card information. The insureds sought a declaratory judgment requiring their insurer to defend and indemnify them in the bank's lawsuit. The court ruled that the bank's claims against the insureds were not covered because the electronically stored cardholder information at issue constituted "electronic data" under the policy, and the policy's coverage for "property damage" – which the policy defined as "[p]hysical injury to tangible property . . . or . . . [l]oss of use of tangible property that is not physically injured" – did not include electronic data by stating that "[f]or the purposes of this insurance, electronic data is not tangible property." *Id.* at 1198. [5]

"Personal and advertising injury".Disputes as to coverage for claims arising from cyber incidents under a CGL policy's "personal and advertising injury" coverage provisions have largely involved claims where electronic data containing personal information was alleged to have been

published in violation of a person's privacy rights. A CGL policy's definition of "personal and advertising injury" typically includes injury arising out of "oral or written publication, in any manner, of material that violates a person's right of privacy," or substantially similar language. Courts have issued divergent opinions as to what constitutes a "publication" for the purpose of coverage for a data breach, particularly on the issues of whether a third party must have viewed the data in order for there to have been a "publication" and whether the insured – as opposed to a third party such as a hacker – must have made the publication in order for there to be coverage.

For example, in *Recall Total Info. Mgmt. Inc. v. Fed. Ins. Co.*, 83 A.3d 664 (Conn. App. Ct. 2014), *aff'd*, 115 A.3d 458 (Conn. 2015), a storage vendor contracted with a technology company to transport and store computer tapes containing personal information of current and former employees of the technology company, and approximately 130 of those tapes were lost when they fell from a truck while being transported by the storage vendor's logistics subcontractor. The lost tapes were removed from the roadside by an unknown individual and never recovered. Although there was no evidence that anyone accessed the information on the tapes or that their loss caused harm to any of the technology company's employees, the technology company incurred over $6 million in expenses in an effort to prevent the employees whose personal information was on the tapes from suffering identity theft, and it sought and received reimbursement of those expenses from the storage vendor. In turn, the storage vendor sought coverage under the logistics subcontractor's CGL policy and umbrella liability policy (which named the storage vendor as an additional insured), but the insurers denied coverage. In the storage vendor's subsequent suit against the insurers for breach of the insurance policies, the storage vendor claimed that the loss constituted a "personal injury" under the policies, which defined "personal injury" as an "injury . . . caused by an offense of . . . electronic, oral, written or other publication of material that . . . violates a person's right of privacy . . . . " However, the court ruled that the policies did not cover the loss because there had not been a "publication" of information resulting in a privacy violation since there was no evidence that the information on the lost tapes was accessed by anyone. *Id.* at 673.

Unlike the court in *Recall*, some courts have determined that there was a "publication" for the purpose of insurance coverage for a data breach even where there was no evidence that a third party viewed the data. For example, in *Travelers Indemnity Co. of America v. Portal Healthcare Solutions, LLC*, 35 F. Supp. 3d 765 (E.D. Va. 2014), *aff'd*, 644 Fed. Appx. 245 (4th Cir. 2016), an insurer sought a declaratory judgment that it did not have a duty to defend its insured, an electronic medical records storage vendor, in a class action filed by patients who alleged that the insured posted their confidential medical records on the internet, making them available to anyone who performed an internet search of a patient's name and clicked on the first result. The insurance policies at issue provided that the insurer was required to pay sums that the insured became legally obligated to pay because of injury arising from: (1) the "electronic publication of material that . . . gives unreasonable publicity to a person's private life" or (2) the "electronic publication of material that . . . discloses information about a person's private life." The court ruled that the insurer had a duty to defend the insured in the patients' class action, and rejected the insurer's contention that that there was no "publication" because no third party was alleged to have viewed the patients' information. [6] In doing so, the court stated that "[p]ublication occurs when information is placed before the public, not when a member of the public reads the information placed before it." *Id.* at 771.

In *Zurich American Ins. Co. v. Sony Corp. of America*, 2014 N.Y. Misc. LEXIS 5141 (Sup. Ct. N.Y. Co. Feb. 21, 2014), the court found that there was a "publication" where hackers obtained customers' personal information, but the court nevertheless ruled that there was no coverage because the publication was not made by the insured. In that case, the insurer sought a declaratory judgment that it did not have a duty to defend the insured in class actions and investigations arising from the 2011 data breach of the Play Station Network and Sony Online Entertainment, in which hackers stole the personal and financial information of approximately 100 million customers. The insured contended that the underlying class actions alleged a covered offense under the policy's "personal and advertising injury" coverage provisions, which included coverage for "oral or written publication, in any manner, of material that violates a person's right of privacy." Despite finding that there was a "publication" once the insured's server sites containing the customer information were intruded, the court held that there was no coverage and that the insurer did not have a duty to defend because the policy's "personal and advertising injury" coverage provisions required the insured to have made the publication in order for there to have been coverage, and could not be expanded to include acts by the third-party hackers. In doing

so, the court also agreed with the insurer's contention that the phrase "in any manner" in the policy's definition of "personal and advertising injury" referred to the "medium" by which data is publicized, such as by fax or email, and not to who makes the publication. *Id*. at **68-72.

Likewise, in a recent federal case decided in November, entitled *Innovak v. Hanover Ins. Co*., 2017 WL 5632718 (M.D. Fla. Nov. 17, 2017), the court agreed with the reasoning of the Sony decision and found that there was no coverage under a CGL policy for a data breach where publication of personal data was not made by the insured. In *Innovak*, the insured – a provider of accounting and payroll computer software systems – sought a declaratory judgment that its insurer was obligated to defend it in an underlying class action in which it was alleged that the insured was the subject of a data breach in which hackers appropriated the underlying plaintiffs' personal private information stored on the insured's software, database and/or portals. The insured contended that there was coverage under the policy's "personal and advertising injury" coverage provisions – which included coverage for "injury, including consequential 'bodily injury', arising out of one or more of the following offenses: . . . e. Oral or written publication, in any manner, of material that violates a person's right of privacy" – since the complaint in the underlying class action alleged that the insured negligently published software that allowed the underlying plaintiffs' personal private information to be known by third parties. The court ruled that there was no coverage for the underlying class action under the "personal and advertising injury" coverage language of the policy because it required the insured to be the publisher of the personal information. In doing so, the court found that the complaint in the underlying class action did not allege that the insured published private information, but instead that the insured "published software." The court further rejected the insured's contention that the phrase "in any manner" in the policy's definition of "personal and advertising injury" connoted both direct publication of personal private information as well as negligent failure to prevent third parties from obtaining the information, as the court agreed with the Sony court's reasoning that the phrase "in any manner" indicates the medium by which data is publicized rather than who makes the publication. [7] *Id*. at **5-7.

Conclusion. As the above cases demonstrate, there is real doubt as to whether a traditional CGL policy can be relied upon to provide coverage for many of the cyber risks that businesses currently face. Adding to that concern are CGL policy endorsements which were made available for insurers' use by the Insurance Services Office in 2014 and, when added to a policy, exclude coverage under a CGL policy for claims arising out of access to or disclosure of confidential or personal information. *See, e.g*., Endorsement CG 21 06 05 14 ("Exclusion – Access or Disclosure of Confidential or Personal Information and Data-Related Liability – With Limited Bodily Injury Exception"). **Therefore, it is important that a business review its CGL and other insurance policies periodically and upon renewal to ensure that they contain language that covers the cyber risks that the business faces and has decided to transfer through insurance, and look into what additional coverage options are available to address gaps in coverage (including cyber insurance policies and cyber-related endorsements to traditional policies).**[8]

Next Client Advisory in this series: Commercial Crime Insurance and Cyber Risk

For more information concerning the matters discussed in this publication, please contact a member of the Cybersecurity Group below or your regular Carter Ledyard attorney.

Mark R. Zancolli (212.238.8735, zancolli@clm.com); **H. Thomas Davis, Jr.** (212.238.8850, davis@clm.com); **John M. Griem., Jr.** (212.238.8659, griem@clm.com); and **Matthew James** (212.238.8644, james@clm.com).

---

[1] NBC News, *Global Cyberattack Hits 150 Countries, Europol Chief Says* (May 14, 2017); NBC News, *'WannaCry' Malware Cyberattack Slows, But Threat Remains, Experts Say* (May 15, 2017).

[2] Consumer Reports, *Equifax Data Breach Affected 2.4 Million More Consumers* (March 1, 2018).

[3] Ponemon Institute, *2017 Cost of Data Breach Study: Global Overview* (June 2017).

[4] CSO Cybersecurity Business Report, *Opinion*, *Top 5 cybersecurity facts, figures and statistics for 2018* (January 23, 2018).

[5] The policy also specifically excluded "[d]amages arising out of the loss of . . . electronic data." *Id*.

[6] In making that contention, the insurer relied on the *Recall* case, but the court found that case to be "distinguishable because, here, the information was posted on the internet and thus, was given not just to a single thief but to anyone with a computer and internet access." *Id*. at 771.

[7] The court further rejected the insured's reliance on *Hartford Casualty Ins. Co. v. Corcino & Assocs., et al*., 2013 WL 5687527 (C.D. Cal. Oct. 7, 2013), a case in which the court dismissed an insurer's action seeking a declaration that it had no obligation to indemnify its insured under a CGL policy's coverage for "personal and advertising injury" with respect to claims against the insured in underlying California state court lawsuits in which the insured was alleged to have violated the privacy rights of numerous patients when it provided the patients' confidential medical data to one of the insured's job applicants to perform certain tasks with the data to test his suitability for employment, and the job applicant proceeded to post the medical data on a public website with a request for help converting the data. The *Innovak* court found the *Corcino* case to be "wholly inapposite" since it "involved allegations that private information was actually posted by the insured, through one of the insured's job applicants, to a public website, which connotes a publication of information," whereas the underlying class action against the insured in *Innovak* did not involve allegations that the insured published private information. *Innovak*, 2017 WL 5632718 at ** 6-7. The coverage dispute in *Corcino* arose from the insurer's contention that there was no coverage for the underlying litigation because it was subject to a policy exclusion that barred recovery for violations of statutorily created privacy rights, but the *Corcino* court rejected that argument by finding that California had recognized both a constitutional privacy right and a common law tort claim for violations of the right of privacy prior to the enactment of the statutes under which the underlying plaintiffs were seeking relief against the insured. 2013 WL 5687527 at **5-6.

[8] Although this series of Advisories will focus on coverage for cyber-related losses under CGL, commercial crime and cyber insurance policies — and cases involving coverage disputes under such policies – coverage for certain types of cyber-related losses may also be found under other policies, such as directors & officers, errors & omissions, kidnap & ransom, and property policies.

related professionals

H. Thomas Davis, Jr. / Partner
D 212-238-8850
davis@clm.com

John M. Griem, Jr. / Partner
D 212-238-8659
griem@clm.com