Legal Insight

K&L GATES

www.klgates.com

May 2013

The text of this article first appeared in the May 2013 issue of *The Insurance Coverage Law Bulletin,* Vol. 12, No. 4

Insurance Coverage for Cyber Attacks

Part One of a Two-Part Article

By Roberta D. Anderson

There's no denying that the present-day Internet, while extraordinary, is increasingly scary. Cyber attacks of various types continue to escalate across the globe. As stated by one recent commentator: "Cybercrime is raging worldwide." Kevin Robinson-Avila, "Cyber attacks on the rise worldwide," *ABQJournal* (Dec. 17, 2012). Reports of highprofile cyber attacks make headlines on an almost daily basis. In recent weeks and months, sophisticated distributed denial-of-service ("DDoS") attacks on at least 26 of the largest U.S. banks reportedly breached some of the nation's most advanced computer security, rendering bank websites unavailable to customers and disrupting transactions for hours at a time.

The headlines confirm the reality: Cyber attacks are on the rise with unprecedented frequency, sophistication and scale. And they are pervasive across industries and geographical boundaries.

While no organization is immune from cyber attacks, it is uncertain that companies are sufficiently aware of the escalating onslaught. Even companies that are sufficiently aware of the problem might not be sufficiently prepared. It is abundantly clear that network security alone cannot entirely address the issue. As noted by one observer: "[t]here is no fail-safe technology that is immune to hacking. Online security will evolve as hackers and security experts work continuously to outwit each other." "The Cloud Darkens," *N.Y. Times* (June 29, 2011).

Insurance can play a vital role. And, yet, some companies may not be adequately considering the important role of insurance as part of their overall strategy to mitigate cyber risk. A recent 2012 survey conducted by global consulting firm Towers Watson reports that 72% of the 153 risk managers of North American companies surveyed "ha[d] not purchased network security/privacy liability policies." 2012 Towers Watson Risk and Finance Manager Survey at p. 1. On the other hand, risk managers and in-house counsel may not be aware if, and to what extent, the company already has coverage for cyber risks under existing "traditional" insurance policies, many of which cover cyber risks.

A complete understanding of the company's insurance program is key to maximizing protection against cyber risk. Indeed, in the wake of "more frequent and severe cyber incidents," the Securities and Exchange Commission's ("SEC") Division of Corporation Finance has issued guidance on cyber security disclosures under the federal securities laws and has advised that companies "should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents" and that "appropriate disclosures may include," among other things, a "[d]escription of relevant insurance coverage." SEC Division of Corporation Finance, Cybersecurity, CF Disclosure Guidance: Topic No. 2 (Oct. 13, 2011).

In view of the cyber risks and realities, companies should carefully examine their insurance programs, evaluate what coverage already may be available, and see what may be done to enhance the available coverage. To the extent that there may be gaps in available coverage, companies should consider how those gaps can be filled, including through specialty "cyber" risk policies.

Cyber Criminals Seize the Day—And the Data

The past two years have seen some of the world's most sophisticated corporate giants fall victim to different types of serious cyber attacks. These attacks have included some of the largest data breaches in history and have affected online gaming providers, marketing services firms, retailers, the health care industry, banks, insurers, defense contractors, social networking sites, cloud storage providers, credit card processors—even sophisticated security firms. The Privacy Rights Clearinghouse reports that, as of March 1, 2013, 607,295,463 records have been breached by 3,669 data breaches made public since 2005. Chronology of Data Breaches: Security Breaches 2005 – Present. The organization notes that "[i]n reality, the number … should be much larger."

The escalating cyber attacks are not limited to data breaches—they also include expensive DDoS attacks, such as the recent attacks that targeted the financial services sector, and myriad other types of cyber threats, including attacks principally designed to destroy or corrupt data, and cyber extortion. The Ponemon Institute's recent *2012 Cost of Cyber Crime Study: United States* concludes that "[c]yber attacks have become common occurrences" with the 56 organizations involved in its survey experiencing "102 [overall] successful attacks per week and 1.8 successful attacks per company per week." *Id.* at 28.

The problem of cyber risks is exacerbated, not only by increasingly sophisticated cyber criminals, malicious code and other types of malware, but also by the reality of the modern business world, which is full of portable devices, including cell phones, laptops, iPads, USB drives, jump drives, media cards, tablets and other devices that facilitate the loss of sensitive information. The Ponemon Institute's recent *2013 State of the Endpoint* study finds that "[o]ne of the top concerns is the proliferation of personally owned mobile devices in the workplace such as smart phones and iPads" and that "data-bearing devices pose a significant security risk to their organization's networks or enterprise systems because they are not secure." *Id.* at 1.

Cyber Attack Costs Are on the Rise

As the incidences of cyber attacks escalate, the costs associated with attacks are also increasing. In data breach cases, companies may incur substantial expenses relating to federal and state notification requirements. In addition to numerous federal statutes and regulations, 46 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information. *See* National Conference of State Legislatures, "State Security Breach Notification Laws" (updated Aug. 20, 2012).

Companies may also face governmental and regulatory investigations, fines and penalties, and lawsuits seeking damages for lost or stolen data, invasion of privacy, misappropriation of intellectual property or confidential business information, or other consequences of a data breach. Even if not ultimately successful, such lawsuits can be extremely costly to defend. Companies may also incur significant expenses associated with retaining forensics experts and assuaging and attempting to maintain customers and curtailing damage to reputation, by, for example, providing credit monitoring services to affected individuals and retaining public relations consultants.

In its seventh annual *2011 Cost of Data Breach Study: United States* published in March 2012, the Ponemon Institute noted that "data breaches continue to have serious financial consequences for organizations." *Id.* at 1. It also is important to note that the study does not include organizations that had data breaches impacting in excess of 100,000 records because they "are not representative of most

data breaches and including them in the study would skew the results." *Id.* But the incidents of largescale breaches are on the rise.

Even in cyber attack cases in which sensitive information is not actually or potentially compromised, a company may experience substantial business interruption and related losses if online systems or websites are disabled by—or disabled in order to address—a cyber attack. A company also may incur damage to its computers, networks, and data, in addition to costs to update and fix any flaws in its security systems. These examples of potential costs and losses are far from exhaustive. The *2012 Cost of Cyber Crime Study: United States* found that "the average annualized cost of cyber crime for 56 organizations in [its] study is $8.9 million per year, with a range of $1.4 million to $46 million." *Id.* at 1. This number is up from the $8.4 million average annualized cost reflected in the 2011 survey.

It is clear that attacks and associated costs are on the rise. And insurance can play an important role in mitigating the problem.

The Role of Insurance

Traditional Insurance Coverages

1) Commercial General Liability Policies

While some companies carry specialty insurance policies that are specifically designed to afford coverage for cyber risk, many companies have various forms of "traditional" insurance policies that may cover cyber risks, including commercial general liability ("CGL") coverage. CGL policies generally cover the company against liability for claims alleging "bodily injury" and/or "property damage" under "Coverage A" and also against liability for claims alleging "personal injury" and/or "advertising liability" under "Coverage B."

Although insurers typically argue that "cyber" risks are not intended to be covered under CGL policies (or other "traditional" types of insurance coverages), insureds pursuing coverage under CGL policies have met with some, albeit not universal, success in pursuing coverage for cyber risks under these policies. Coverage in a particular case necessarily will depend on the specific facts of each case, the terms, conditions and exclusions of each individual policy, and the applicable law.

A brewing legal dispute between Sony and one of its insurers concerning the PlayStation Network data breach highlights the challenges that companies can face in getting insurance companies to cover losses arising from cyber risks under CGL policies. In *Zurich American Insurance Co., et al. v. Sony Corp. of America, et al.*, No. 651982/2011 (N.Y. Sup. Ct. New York Cty.) (filed July 20, 2011), the insurer seeks a declaration that there is no coverage under the CGL policies at issue on the basis that the underlying lawsuits arising out of the cyber attacks "do not assert claims for "bodily injury," "property damage" or "personal and advertising injury." Complaint at ¶ 28. The Sony coverage litigation may provide additional guidance on the scope of coverage for data breaches and other cyber risks under traditional CGL policies. In the meantime, the current case law is instructive.

2) Potential Coverage Under Commercial General Liability Policies

Electronic Data As "Property" Subject to Damage: The main coverage part of the current standard Insurance Services Office, Inc. ("ISO") CGL policy form states that the insurer "will pay those sums that the insured becomes legally obligated to pay as damages because of 'bodily injury' or 'property damage,'" which "occurs during the policy period." ISO Form CG 00 01 04 13 (2012), Section I, Coverage A, §§ 1.a.,1.b.(2).

Insurance Coverage for Cyber Attacks

One potential issue in cyber risk cases is whether the definition of "property damage" is satisfied. A standard form definition of "property damage" includes "[p]hysical injury to tangible property, including all resulting loss of use of that property" and "[l]oss of use of tangible property that is not physically injured." Section V, § 17. The standard form further states that the insurer "will have the right and duty to defend the insured against any 'suit'" seeking potentially covered damages. Section I, Coverage A, § 1.a.

Insurers typically argue that data is not "tangible property" that can suffer "physical injury" and, therefore, is not "property damage" as defined in the policy. However, a number of courts have disagreed holding that damaged or corrupted software or data is "tangible property" that can suffer "physical injury." For example, the Court of Appeals of Minnesota in *Retail Systems, Inc. v. CNA Insurance Co.*, 469 N.W.2d 735 (Minn. Ct. App. 1991), *review denied* (Aug. 2, 1991), found that "data on [a] tape was of permanent value and was integrated completely with the physical property of the tape." *Id.* at 737. On this basis, the court held that both "the computer tape and data are tangible property" and, therefore, can be the subject of covered "property damage." *Id.*

Consistent with the holding in *Retail Systems*, the District of Arizona in *American Guarantee & LiabilityInsurance Company v. Ingram Micro, Inc.*, 2000 WL 726789 (D. Ariz. Apr. 18, 2000), held that electronic data can suffer "physical injury." As stated by the court:

> At a time when computer technology dominates our professional as well as personal lives, the Court must side with [the insured]'s broader definition of 'physical damage.' The Court finds that 'physical damage' is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality. *Id.* at *2.

In support of its holding, the *Ingram Micro* court cited to various state and federal laws that make it a crime to cause "damage" to computer hardware or data, noting that "[l]awmakers around the country have determined that when a computer's data is unavailable, there is damage; when a computer's services are interrupted, there is damage; and when a computer's software or network is altered, there is damage." *Id.* at *3. Although *Ingram Micro* concerned an all-risk policy, the decision clearly holds that data is tangible and can therefore suffer "physical injury."

Other courts likewise support an argument that data is tangible property. The decisions are not uniform, however, and some courts have held that computer data is not tangible property and therefore is not susceptible to property damage. *See, e.g., Ward General Ins. Services, Inc. v. Employers Fire Ins. Co.*, 7 Cal.Rptr.3d 844, 851 (Cal. App. Ct. 2003). A leading insurance law authority notes that the issue as to whether "computerized information is tangible property" has "not been satisfactorily resolved." 9 Couch on Insurance § 126:40 (3d ed. 2012).

One potential hurdle for insureds is that the current ISO standard form CGL policy, and other ISO standard form CGL policies written or effective on or after Dec. 1, 2001, expressly exempt "electronic data" from the definition of "property damage." In addition, standard form CGL policies effective on or after Dec. 1, 2004 expressly exclude "[d]amages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." ISO Form CG 00 01 04 13, Section I, Coverage A, § 2.p.

It is important to recognize that the various limitations and exclusions may not vitiate coverage. For example, the ISO "Electronic Data Liability" Endorsement adds "electronic data" back to the definition of "property damage." ISO Form CG 04 37 12 04 (2003). Standard form ISO policies written or effective on or before Dec. 1, 2001, moreover, do not except "electronic data" from the definition of "property damage" and do not exclude "electronic data." Even recently issued policies

may not contain such exceptions or exclusions. One might reasonably presume, for example, that the Zurich policies in the Sony PlayStation coverage litigation, which are alleged to be effective for the policy period beginning April 1, 2011, do not contain any express exceptions or exclusions — none are raised in Zurich's complaint.

Even where a policy contains an express "electronic data" exclusion some courts have found coverage. For example, the Eighth Circuit in *Eyeblaster, Inc. v. Federal Ins. Co.*, 613 F.3d 797 (8th Cir. 2010), held that an insurer had a duty to defend a complaint alleging injury to the plaintiff's "computer, software, and data after [the plaintiff] visited [the insured's] website." *Id.* at 799. The plaintiff alleged that "his computer was infected with a spyware program from [the insured] on July 14, 2006, which caused his computer to immediately freeze up" and that "he lost all data on a tax return on which he was working and that he incurred many thousands of dollars of loss." *Id.* at 800. The plaintiff further alleged that "he ha[d] experienced the following: numerous pop-up ads; a hijacked browser that communicates with websites other than those directed by the operator; random error messages; slowed computer performance that sometimes results in crashes; and ads oriented toward his past web viewing habits." *Id.* The insured's CGL policy obligated "the insurer to provide coverage for property damage caused by a covered occurrence." *Id.* at 801. "Property damage" was defined in the policy at issue as "physical injury to tangible property, including resulting loss of use of that property …; or loss of use of tangible property that is not physically injured." *Id.* The definition of tangible property" excluded "any software, data or other information that is in electronic form." *Id.*

Notwithstanding the express exclusion, the court held that the insurer was obligated to defend because the complaint alleged "loss of use of tangible property that is not physically injured" under the second prong of the "property damage" definition. As the court concluded, "The plain meaning of tangible property includes computers, and the [underlying] complaint alleges repeatedly the 'loss of use' of his computer. We conclude that the allegations are within the scope of the General Liability policy." *Id.* at 801-02. As claims increase, we can expect to see more courts addressing whether such claims raise sufficient issues to at least trigger a defense obligation under the CGL Coverage A.

"Publication" That Violates a"Right of Privacy": The "Personal And Advertising Injury Liability" coverage part of the current standard form ISO CGL policy states that the insurer "will pay those sums that the insured becomes legally obligated to pay as damages because of 'personal and advertising injury,' which is caused by an offense arising out of [the insured's] business." ISO Form CG 00 01 04 13 (2012), Section I, Coverage B, §§ 1.a., 1.b. "Personal and advertising injury" is defined in the ISO standard form policy to include a list of specifically enumerated offenses, which include the "offense" of "[o]ral or written publication, in any manner, of material that violates a person's right of privacy." Section V, § 14.e. Similar to Coverage A, the policy further states that the insurer "will have the right and duty to defend the insured against any 'suit.'" Section I, Coverage B, § 1.a. The CGL Coverage B can indemnify and provide a defense against a wide variety of claims, including claims alleging violation of privacy rights.

Potential issues arising under Coverage B include whether there has been a "publication" that violates the claimant's "right of privacy"—both terms are left undefined in standard form ISO policies. Courts generally have construed these requirements favorably to insureds, and this coverage may afford broad coverage to companies for theft of consumer data and misuse of customer information, copyright infringement and other types of unfair competition. For example, in *Tamm v. Hartford Fire Insurance Co.*, 2003 WL 21960374 (Mass. Super. Ct. 2003), the Superior Court of Massachusetts confirmed that the insurer had a duty to defend a lawsuit alleging, *inter alia*, that the insured "access[ed] and distribut[ed] information obtained in private email accounts" and "threatened to contact a list of specific e-mail addresses for individuals … " *Id.* at *2. The underlying lawsuit set out

10 counts against the insured, including "violations of RICO, misappropriation of trade secrets, and violations of Federal wiretapping laws" and requested that "the court restrain [the insured] from 'disclosing to any person or entity, or using in any other manner, any confidential or proprietary information or materials belonging to or wrongfully acquired from [the plaintiff] or its officers, directors, employees, attorneys, or agents.'" *Id.* at *3. Based on the complaint, the court easily concluded that the insurer had a duty to defend under the insurance policy. As the court reasoned:

> In order to trigger the duty to defend under the invasion of privacy language of the policy, an underlying complaint must allege two things: (1) an "oral or written publication" of (2) "materials that violate person's rights of privacy." The [underlying] complaint alleges that [the insured] accessed the private e-mail accounts of [the plaintiff] and its executives and sent these private communications and materials to several outside counsel for [the plaintiff]. The allegations of sending these private communications via e-mail to outside attorneys seemingly satisfies both prongs under the invasion of privacy clause of the policy. *Id.*

More recently, the Ninth Circuit upheld coverage in *Netscape Communications Corp. v. Federal Ins.Co.*, 343 Fed.Appx. 271 (9th Cir. 2009). In that case, the underlying plaintiffs alleged that the insured's "SmartDownload [software] violated the claimants' privacy by, among other things, collecting, storing, and disclosing to Plaintiffs and their engineers claimants' Internet usage." 2007 WL 1288192, at *1 (N.D. Cal. Apr. 27, 2007). The insurance policy obligated the insurer to "pay amounts [the insured] is legally required to pay as damages for covered personal injury that … is caused by a personal injury offense," which was defined to include the offense of "[m]aking known to any person or organization written or spoken material that violates a person's right to privacy." 2007 WL 2972924, at *2 (N.D. Cal. Oct. 10, 2007), *aff'd in part, rev'd in part*, 343 Fed.Appx. 271 (9th Cir. 2009). The court held that the insurer had a duty to defend, reasoning that "when [the insured] received information from SmartDownload, it was making it known to AOL by transmitting it to its parent company. Similarly, individual [insured] employees made the information known to each other by circulating files among themselves with the information gained from SmartDownload." *Id.* at *6, 343 Fed.Appx. at 271. The Ninth Circuit affirmed that "the district court correctly determined that the claims against [the insured] were 'personal injury offenses' and within the policy's coverage." 343 Fed.Appx. at 271.

Again, there may be potential coverage hurdles under Coverage B. ISO standard form policies written or effective on or after Dec. 1, 2001 contain exclusions relating to Internet-related activities that insurers may assert to limit the broad grant of coverage. The ISO policies written or effective on or after Dec. 1, 2001, for example, contain exclusions relating to Internet activities. *See* ISO Form CG 00 01 12 07 (2007), Section I, Coverage B, § 2.j., k. Unless clear and unambiguous, however, any exclusions should be construed in favor of the insured pursuant to established canons of insurance policy construction. 2 Couch on Insurance 3d § 22:31 (2012) ("provisos, exceptions, or exemptions, and words of limitation in the nature of an exception ... are strictly construed against the insurer …"). Whether an exclusion applies will depend upon the specific exclusionary language in the policy and whether the insurer can meet its burden to demonstrate that the exclusion applies to the loss in question under applicable law.

Insurance Coverage for Cyber Attacks

Author:

Roberta D. Anderson
roberta.anderson@klgates.com
+1.412.355.6222

K&L GATES

Anchorage Austin Beijing Berlin Boston Brisbane Brussels Charleston Charlotte Chicago Dallas Doha Dubai Fort Worth Frankfurt Harrisburg Hong Kong Houston London Los Angeles Melbourne Miami Milan Moscow Newark New York Orange County Palo Alto Paris Perth Pittsburgh Portland Raleigh Research Triangle Park San Diego San Francisco São Paulo Seattle Seoul Shanghai Singapore Spokane Sydney Taipei Tokyo Warsaw Washington, D.C. Wilmington

K&L Gates practices out of 48 fully integrated offices located in the United States, Asia, Australia, Europe, the Middle East and South America and represents leading global corporations, growth and middle-market companies, capital markets participants and entrepreneurs in every major industry group as well as public sector entities, educational institutions, philanthropic organizations and individuals. For more information about K&L Gates or its locations, practices and registrations, visit www.klgates.com.