Insurance Coverage Litigation
FROM THE SECTION OF LITIGATION INSURANCE COVERAGE LITIGATION COMMITTEE
March-April 2014, Vol. 24 No. 2

Cyber Risk Coverage Litigation Heats Up as Exposure and the Insurance Market Evolve

By Gregory D. Podolak[1]

You may have heard . . .

- A phishing email to a heating, ventilation, and air-conditioning contractor caused the Target data breach of 110 million records.
- A five-year-old successfully hacked Microsoft's Xbox Live.
- Two-thirds of the entire Internet has been exposed to an undetected security leak since March 2012 (Heartbleed).

Cyber risk is dominating the headlines and has become a mainstay in the world of corporate risk management. It is incumbent on risk managers, general counsel, and chief information/security officers to appreciate the risk and be conversant in the legal landscape and ever-evolving cyber insurance marketplace in order to effectively assess and tailor their insurance program to match the growing threat.

Cyber Risk: The Exposure

The term "cyber risk" is somewhat amorphous and continues to develop as the nature of technology expands, but it generally includes any loss exposure associated with the use of electronic equipment, computers, information technology, and virtual reality. The data breach is perhaps the most prevalent, widely publicized, and expensive exposure today. In the case of individuals, a data breach involves stolen "personally identifiable information," such as credit card information and Social Security numbers, or "personal health information," such as medical records. For corporations, it can involve various forms of sensitive or confidential information, such as client records, bid data, trade secrets, financial records, and litigation information. Hacking and malicious intrusions are usually the cause of the breach, but human error is just as prevalent a concern. A 2013 study by the Ponemon Institute found that, globally, 64 percent of all breaches are caused by some form of human error[2]—inadequate data security; system glitches; and simple, routine carelessness (such as losing an unencrypted company laptop).

The exposure to data breaches is so pervasive and costly that 2013—which saw a 62 percent increase in the total number of breaches from 2012, globally, and the exposure of 552 million identities—was dubbed the year of the "mega breach."[3] The exposure continues to widen, as data thieves look to exploit less traditional conduits of information, such as mobile devices (through mobile malware and text messaging phishing schemes), security cameras, smart televisions, automobiles, and even baby monitors.[4] It appears that this trend will only continue. The first quarter of 2014 has already seen the following:[5]

- AIG's Variable Annuity Life Insurance Company disclosed that a former financial advisor took a hard drive with information related to 774,723 customers.

- The Archdiocese of Seattle revealed that hackers had struck its database, exposing an estimated 90,000 records related to employees and volunteers.

- The Los Angeles Department of Health Services is notifying approximately 168,000 patients that personal health information and billing information was at risk of exposure after its third-party billing/collections vendor, Sutherland Healthcare Solutions, had computer equipment stolen from its office.

- The Internal Revenue Service stated that an employee took home personal information on about 20,000 individuals stored on a drive and loaded it onto an unsecure home network.

- Coco-Cola said that a former employee in Atlanta stole 55 laptops that contained unencrypted personal information of almost 74,000 people, mostly employees.

- Sally Beauty Holdings disclosed that hackers broke into its network and stole credit-card data on an estimated 25,000 customers.

- Banner Health accidently exposed Medicare and Social Security information of more than 50,000 people on magazine address labels.

- Assisted Living Concepts, which operates care facilities in 20 states, disclosed that hackers breached a vendor's system, gaining access to payroll files on 43,600 current and former employees.

- Home Depot in Atlanta said three human resources employees were charged with stealing confidential information regarding 20,000 coworkers and opening fraudulent credit cards.

Cyber risks cause both first-party losses, suffered directly by the affected individual or company, and third-party liability claims brought by others against the policyholder. First-party losses typically include forensic investigation expenses, replacement costs for hardware and/or software, and business interruption losses. In 2012, United States businesses suffered a combined $3.03 million in lost-business costs resulting from data breaches.[6] Data breaches also typically result in costs associated with providing notice of a breach, credit monitoring, public relations consultants, payment of fines and penalties, and compliance with governmental or regulatory investigations. Forty-six states have security breach notification laws when certain types of personally identifiable information have been compromised.[7]

Cyber risks can also result in a variety of individual and class action third-party liability claims for property damage, invasion of privacy, bodily injury, and/or emotional distress. It is also likely to mean claims by the government. In response to overwhelming consumer exposure, federal oversight is increasing and becoming increasingly complex. The Federal Trade Commission (FTC) leads the regulatory charge, routinely pursuing claims of "unfair or deceptive" practices affecting commerce against companies that fail to provide adequate data security. The FTC's authority in the cyber arena is only expanding. While many FTC targets choose to settle out of court—Facebook famously did so in 2011, for example—one company recently disputed the FTC's authority to police data security issues. Before a federal district court in New Jersey, Wyndham Worldwide Corporation argued that Congress never intended the FTC to have data security oversight. In its April 7, 2014, ruling, the court disagreed with Wyndham and refused to carve out a data security exception from the FTC's province, holding that subsequent data-security legislation actually complements the FTC's authority.[8]

Cyber Risk Insurance Litigation

Meanwhile, courts have been regularly weighing in on cyber-related insurance disputes, with several key decisions coming within the last six months and establishing the parameters of the legal landscape for coverage of cyber risks.

Current issues in commercial general liability. Historically, commercial general liability (CGL" insurance is the most common type of coverage found in most insurance programs, and policyholders will invariably look to this as a first source of recovery. The problem: CGL insurers don't view CGL insurance as intending to cover cyber risks and vigorously deny owing any obligation for them. Over the years, the debate has produced litigation on two key fronts: whether there is "property damage"[9] or "personal injury."[10]

For example, a court found property damage where a power outage knocked out computer systems for an entire day and caused a loss of data and software functionality in *American Guaranty & Liability Insurance Co. v. Ingram Micro, Inc.*[11]. Similarly, damage to a computer caused by "freezing," slowed operations, and a hijacked browser was considered property damage in *Eyeblaster, Inc. v. Federal Insurance Co.*[12] An Internet service provider's interception and internal dissemination of its users' online activities for advertising purposes qualified as personal injury (breach of privacy) in *Netscape Communications Corp. v. Federal Insurance Co.*[13]

Recent case law suggests the debate on these issues is evolving, policyholders are pursuing coverage under alternate lines of coverage, and insurers are aggressively denying claims as the market transitions to dedicated cyber coverage.

When is compromised data considered published? On January 14, 2014, the Connecticut Appellate Court decided *Recall Total Information Management v. Federal Insurance Co.*,[14] in which a third-party storage vendor lost 130 IBM data

tapes that included personal information for 500,000 IBM employees. The tapes literally "fell off the back of a truck" while in transit, were taken by an unknown person, and were never recovered.

Recall, the vendor, paid IBM $6 million for costs and expenses resulting from the loss of the tapes—notification to affected individuals, establishing a call center for inquiries, credit monitoring and restoration—and pursued CGL coverage.[15] Recall argued that the loss of the tapes qualified for personal injury coverage, which insured "injury, other than bodily injury, property damage or advertising injury, caused by an offense of . . . electronic, oral, written or other publication of material that . . . violates a person's right to privacy." The court held that, even though the tapes and otherwise private data stored on them were no longer in the exclusive control of those entrusted with them, there was no "publication" because there was no evidence the data on the tapes had ever been accessed. The court's conclusion was unaffected by the fact that IBM was required to take action under relevant state security breach notification laws, reasoning that such statutes can be triggered by the need for preventive action and do not necessarily reflect that a privacy breach has actually occurred. Recall appealed the ruling, and the Connecticut Supreme Court accepted certification on March 5, 2014.

One month after *Recall*, on February 21, 2014, a New York trial court added a new wrinkle to the "publication" debate, questioning *who* published the information. In *Zurich American Insurance Co. v. Sony Corp. of America*,[16] Sony sought CGL "personal injury" coverage following a hack of its PlayStation Network that resulted in stolen personal information belonging to 100 million users. Zurich argued that the relevant policy language "oral or written publication in any manner of material that violates a person's right of privacy" requires that the publication be made by the insured. Because hackers stole the information, Zurich argued, there was no publication by Sony and thus no coverage. The court agreed.

The court's decision is surprising, given that the relevant language makes no mention of who must make the publication ("any manner" will suffice); and the underlying class action suit against Sony alleged that Sony's lax security measures permitted the hackers to gain access to the network, meaning that Sony arguably was responsible for the publication and should at least have triggered the duty to defend. It is interesting that, before announcing its ruling, the court reportedly told the parties that the insurance issues were important enough to require "immediate appellate authority."[17] Sony appealed the decision on April 9, 2014.

Not all government action constitutes excluded statutory violations. Given the considerable government interest in regulating privacy violations and data security, insurers have also been denying coverage on exclusions relating to statutory violations. Such was the case before a federal district court in California in *Hartford Casualty Insurance Co. v. Corcino & Assocs.*,[18] in which Stanford Hospital sought coverage for litigation brought by numerous patients alleging privacy rights violations. Specifically, the underlying plaintiffs alleged that Stanford and others

posted confidential medical information on a public website in violation of their constitutional privacy rights and California's Confidentiality of Medical Information Act. The plaintiffs also claimed statutory damages under California's Welfare and Institutions Code.

The CGL policy at issue covered "electronic publication of material that violates a person's right of privacy" but excluded any such injury "arising out of the violation of a person's right to privacy created by any state or federal act." The exclusion would not apply, however, to "liability for damages that the insured would have in the absence of such state or federal act." After examining relevant legislative history, the court held that the exclusion did not apply because the statutes at issue did not create new privacy rights; they merely codified and created an enforcement mechanism for existing rights.

The Federal District Court for the Western District of Washington faced a similar dispute in the more recent decision of *National Union Fire Insurance v. Coinstar*.[19] In its ruling, the court held that alleged violations of the Video Privacy Protection Act (VPPA)[20] fell within an exclusion for "any act that violates a statute . . . that addresses or applies to the sending, transmitting or communicating of any material or information, by any means whatsoever." Specifically, the underlying plaintiffs alleged that Coinstar retained consumer personally identifiable information it had obtained through its Redbox system for marketing purposes and disclosed the information to third parties without the consumers' express permission. The court found the exclusion unambiguous and that it applied to the alleged VPPA violations.

Coinstar may be an anomalous ruling, as many versions of the exclusion addressed in that case are specifically limited to violations involving the Telephone Consumer Protection Act, CAN-SPAM,[21] and the Fair Credit Reporting Act. In fact, Coinstar unsuccessfully argued that its version of the exclusion was likewise limited because prior policies expressly referred to those statutory schemes. With that in mind, the *Coinstar* decision provides two important cyber risk lessons for policyholders: (1) Given the prominence of government intervention in data breach losses, insurers may attempt to take advantage of any exclusion pertaining to statutory violations; and (2) at the time of renewal, policyholders should take care to avoid unnecessarily broad exclusions pertaining to statutory violations or government regulations.

First-party insurance may be available.

Property insurance: Does the policy contemplate electronic losses? Policyholders are also facing coverage disputes on the first-party front. On November 21, 2013, a federal district court in Georgia analyzed first-party property insurance in *Metro Brokers, Inc. v. Transportation Insurance Co.*.[22] In *Metro*, a real estate broker's (Metro's) online banking system was hacked by a thief who fraudulently authorized Automated Clearing House payments from one of Metro's client escrow accounts to several banks throughout the United States. Metro's first-party property insurance covered "direct physical loss of or damage to Covered Property . . . caused by or resulting from a Covered Cause of Loss" and included a coverage extension for

"forgery." The policy excluded losses involving "malicious code" and "system penetration." The court found there was no coverage for two reasons.

First, the electronic transfers did not meet the insuring agreement definition of "forgery" because they did not qualify as "a check, draft, promissory note, bill of exchange, or similar written promise, order, or direction to pay a sum certain." The court characterized the "forgery" definition as applying only to so-called "traditional" negotiable instruments and distinguished the policyholder's loss as involving an electronic transfer. Essentially, the court was drawing a line between physical instruments and those commenced by "the click of a button and series of electronically transmitted codes."[23]

On concluding that the insuring agreement had not been met, the court's analysis could have ended. However, it went on to discuss the exclusions. Metro argued that neither should apply because the theft was proximately caused by a person (or persons); the computer virus was merely a tool those person(s) used to commit the theft. Unfortunately, the exclusions, which the court described as "extraordinarily broad," were preceded by anti-concurrent language[24] that effectively defeated Metro's argument.

Crime insurance: Common data breach damages are proximately caused by hacking. In 2012, the Sixth Circuit Court of Appeals considered whether the theft of credit card information from a retailer is covered under crime insurance. In *Retail Ventures, Inc. v. National Union Fire Insurance Co.*,[25] hackers used the local wireless network at one DSW retail store to access DSW's main computer system and download credit card and checking account information of 1.4 million customers from 108 stores. DSW suffered losses relating to customer communications, public relations, customer claims and lawsuits, and attorney fees in connection with state and federal investigations. DSW sought $6.8 million[26] from AIG under the "Computer Fraud Rider" of its crime insurance. The rider insured loss "resulting directly from" the theft of insured property by computer fraud.

In its attempt to deny coverage, AIG first argued that the court should interpret the "resulting directly from" language narrowly to mean "solely" and "immediately," thus precluding coverage for the majority of DSW's damages. The Sixth Circuit disagreed and applied a proximate cause standard, agreeing with the district court that "there is a sufficient link between the computer hacker's infiltration of Plaintiffs' computer system and Plaintiffs' financial loss" to trigger coverage.[27]

AIG also argued the loss was excluded as "loss of proprietary information, Trade Secrets, Confidential Processing Methods, or other confidential information of any kind." The court disagreed and held that the stolen customer information was not DSW's confidential information, but was obtained from customers in order to receive payment and did not involve the manner in which the business is operated. Because the loss was not "clearly excluded," DSW was entitled to coverage.

The Cyber Market

Cyber risks are being pushed out of traditional lines. In addition to aggressively denying coverage under traditional lines, the insurance market is continuing an effort to modify standard coverage terms to eliminate the debate prospectively.

In 2001, the Insurance Services Office (ISO) amended the definition of property damage to specifically omit coverage for "electronic data" and, in 2004, added an exclusion for "[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." Although courts interpret exclusions narrowly, "arising out of" is usually broadly defined. It is important to note that ISO offers an endorsement that carves "damages because of property damage" out of the exclusion (CG 04 37 12 04); the 2013 version (CG 04 37 04 13) also excepts bodily injury claims. Similar "electronic" exclusions are also becoming mainstays of property policies; electronic data are often specifically identified as excluded "property." In 2013, ISO also introduced an optional endorsement (CG 24 13 04 13) that would modify the "personal and advertising injury" definition to eliminate the key coverage on which data breach claims are routinely based: "oral or written publication, in any manner, of material that violates a person's right of privacy."

More is on the way. In May 2014, ISO will make available a new endorsement entitled "Access or Disclosure of Confidential or Personal Information and Data Related Liability—with Limited Bodily Injury Exception." This exclusion eliminates coverage for

> damages arising out of: (1) any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information, or any other type of nonpublic information; (2) or [t]he loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data. [28]

This modified language will pose a considerable hurdle to obtaining CGL coverage for cyber risks—and data breaches, in particular. The savvy policyholder will want to carefully scrutinize its insurance policies to see if the endorsement is added.

Dedicated cyber lines need careful examination. At the same time, there has been a significant increase in stand-alone cyber policies hitting the marketplace. In general, these are viable, commonsense alternatives to traditional policies. However, these policies are still relatively new and untested, so it will be some time before courts have an opportunity to rule on any new concepts and language they might introduce. In fact, "cyber insurance" has only existed since the late 1990s, when the focus was primarily on Y2K conversion concerns. Today, some 50–70 different insurers are writing policies and ISO has crafted its own product.

With so much diversity in an emerging marketplace, it is important to remember that these policies usually are not one-size-fits-all. In fact, the purported coverages can vary dramatically, often being tailored to a particular type of risk or industry, such as financial, technology, or advertising. Examples include website publishing, security breach liability, programming errors and omissions, replacement of electronic data, and business income. Some only cover first party losses, others only third party losses. Some provide defense; some provide only indemnity.

It is also important to scrutinize key terms prior to placement. For example, some policies define covered personally identifiable information by reference to specific statutory schemes, regulations, or both. However, the privacy breach notification arena is rapidly evolving, and many of these statutory schemes are changing. Nineteen states have introduced or are considering revisions to privacy breach legislation in 2014.[29] Policyholders will also need to be sure they have coverage for liability associated with handling the data of others, not just data in their own immediate possession. Fazio Mechanical Services, Inc., the HVAC contractor whose electronic billing connection to Target led to the now infamous data breach, is a prime example of the substantial loss that can emanate even from seemingly mundane electronic connections.

Any policyholder investigating a cyber risk policy will need to fully vet and understand its unique risk exposure; consultation with a knowledgeable broker, legal counsel, and a seasoned information technology professional is a must.

Conclusion

Insurance coverage for cyber risks under traditional coverage lines has been hotly litigated over the past decade, and insurers are increasingly attempting to move cyber risks to dedicated policies. Coverage under traditional policies will be increasingly difficult to access. Despite this momentum, traditional insurance policies may still be available to respond to cyber losses, and policyholders should always carefully assess the nature and extent of a loss and critically evaluate policy terms. Above all else, policyholders should be proactively assessing their cyber coverage needs.

Keywords: litigation, insurance, coverage, cyber risk, security breach, data breach, policyholder

Gregory D. Podolak is with Saxe Doernberger & Vita, P.C.

[1] Gregory D. Podolak is a partner at Saxe Doernberger & Vita, P.C., where he exclusively represents insurance policyholders, advising corporate clients on

insurance recovery/litigation and policy renewal strategy for all lines of coverage. Greg leads SDV's Cyber Risk concentration.

[2] Ponemon Inst., *2013 Cost of Data Breach Study: Global Analysis* 7 (May 2013).

[3] Symantec Corp., *2014 Internet Security Threat Report* 5 (Apr. 2014).

[4] Symantec Corp., *2014 Internet Security Threat Report* 7 (Apr. 2014).

[5] Ellen Messemer, "The Worst Data Breaches of 2014 . . . So Far (Q1)," *NetworkWorld*, Apr. 8, 2014.

[6] Ponemon Inst., *2013 Cost of Data Breach Study: Global Analysis* 17 (May 2013).

[7] Nat'l Conference of State Legislatures, State Security Breach Notification Laws (Jan. 21, 2014).

[8] *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, 2014 U.S. Dist. LEXIS 47622, *25–26 (D.N.J. Apr. 7, 2014).

[9] The standard CGL Coverage A insuring agreement provides: "We will pay those sums that the insured becomes legally obligated to pay as damages because of 'bodily injury' or 'property damage' to which this insurance applies." "Property damage" means, in relevant part, "physical injury to tangible property" and "loss of use of tangible property that is not physically injured." *See* Insurance Services Office (ISO) Form CG 00 01 12 04.

[10] The Coverage B insuring agreement provides: "We will pay those sums that the insured becomes legally obligated to pay as damages because of 'personal and advertising injury' to which this insurance applies." "Personal and advertising injury" means, among other things, "oral or written publication, in any manner, of materials that violates a person's right of privacy."

[11] 2000 U.S. Dist. LEXIS 7299 (D. Ariz. 2000).

[12] 613 F.3d 797 (8th Cir. 2010). *But see Am. Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89 (4th Cir. 2003) (holding that software and data were not "tangible property" and concluding that any "loss of use" would be excluded).

[13] 343 F. App'x 271 (9th Cir. 2009). *See also Zurich Am. Ins. Co. v. Fieldstone Mort. Co.*, 2007 U.S. Dist. LEXIS 81570 (D. Md. 2007) (holding that under the CGL policy's advertising injury definition, "publication" did not need to be to a third party; the perpetrators' wrongful access to the information was sufficient).

[14] 147 Conn. App. 450 (2014).

[15] Recall was an additional insured on a CGL policy procured by its subcontractor, Executive Logistics. Recall also pursued a contractual indemnity claim against Executive Logistics and, after the insurers denied coverage, acquired Executive Logistics' rights under the policy.

[16] No. 651982/2011 (N.Y. Sup. Ct. 2014).

[17] Bibeka Shrestha, "Sony Fights Ruling that Nixed Data Breach Coverage," *Law360*, Apr. 11, 2014.

[18] 2013 U.S. Dist. LEXIS 152836 (C.D. Cal. Oct. 7, 2013).

[19] 2014 U.S. Dist. LEXIS 31441 (W.D. Wash. Feb. 28, 2014).

[20] The VPPA "prohibits a 'video tape service provider' from disclosing [to any person] 'personally identifiable information' about one of its consumers." 2014 U.S. Dist. LEXIS 31441, at *8.

[21] CAN-SPAM is short for the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2013.
[22] 2013 U.S. Dist. LEXIS 184638 (N.D. Ga. Nov. 21, 2013).
[23] *Metro Brokers, Inc.*, 2013 U.S. Dist. LEXIS 184638, at *16.
[24] A clause customarily seen in first-party policies that is intended to exclude a loss even when caused by a combination of both covered and excluded causes of loss.
[25] 691 F.3d 821 (6th Cir. 2012).
[26] $5.3 million in stipulated losses incurred by the plaintiffs, plus $1.49 million in prejudgment interest.
[27] *Retail Ventures, Inc.*, 691 F.3d at 828.
[28] *See* ISO Form CG 21 07 05 14.
[29] Nat'l Conference of State Legislatures, 2014 Security Breach Legislation (Apr. 7, 2014).