

A Watershed Moment for Cyberinsurance

Of the many cyberattacks in 2014, none was as sensational as the November 2014 catastrophic attack waged by The

Guardians of Peace on Sony Pictures Entertainment's computer systems. The hackers stole 100 terabytes of data, including personal identification information ("PII") (e.g., social security numbers, email addresses, employee IDs, medical records, and financial information) belonging to more than 47,000 of Sony's current and former employees. The PII was subsequently "dumped" on various Internet sites and downloaded repeatedly. American intelligence officials tied the attack to the government of North Korea, which was allegedly upset by Sony's release of *The Interview*, a movie starring James Franco and Seth Rogen, in which they are recruited by the United States government to assassinate Kim Jong-un, the Supreme Leader of North Korea.

This breach had all the hallmarks of other headline-grabbing breaches. What made this breach truly sensational, however, was not the number of compromised records—the breach was not even one of the largest breaches in 2014 in terms of records breached. See Cammy Harbison, "10 Largest Data Breaches of 2014; The Sony Hack Is Not One of Them!", *iDigitalTimes.com*, Dec. 26, 2014. Rather, *The Interview*

Attack had all the trappings of a Hollywood movie. It had espionage, a threat against a major motion picture studio, and the release of confidential, embarrassing, and proprietary information and intellectual property.

Experts estimate Sony's response costs at well over \$100 million. *Reactions*, "Sony Pictures Says Cyber Attack Fully Insured," Jan. 9, 2015. Sony smartly had the foresight to purchase a \$60 million cyberinsurance program. See Melissa Hillebrand, "Sony Pictures Holds \$60 Million Cyber Policy with Marsh," *Property Casualty 360*, Dec. 18, 2014. Other small-, medium-, and larger-sized businesses are not so fortunate or well prepared. Instead, they still rely on commercial general liability ("CGL") insurance. This mistaken reliance on CGL policies is problematic, as courts across the country have begun to address disputes between insureds and their CGL insurers arising out of data breach tenders and are confirming a lack of coverage for these types of exposures. For instance, the 2014 *Zurich v. Sony* decision from a New York Supreme Court (which is presently on appeal) found that Sony's insurers had no duty to defend or indemnify in connection with the 2011 attack on Sony's online gaming networks. Additionally, ISO recently introduced broad privacy-related endorsements clarifying the intent that CGL policies were never intended to and do not cover data breach exposures, thus eliminating any arguments to the contrary.

Insurance industry experts have aptly described *The Interview* Attack as a "watershed event" for cyberinsurance. See *Business World*, "Cyber-Risk Insurance Is Hard To Find," Dec. 22, 2014. It also has been described as "a wake-up call for companies" that have an online presence or store sensitive personal or corporate information to embrace cyberinsurance. See Louisa Esola, "North Korea's Sony Hack Seen as Cyber Security Game-Changer," *Business Insurance*, December 21, 2014.

This article analyzes the emerging cyberinsurance market and the options available to protect companies of all sizes from data breach losses. The authors discuss why traditional CGL policy forms were never designed to, and do not, cover these exposures. We conclude by reviewing the essential and ongoing risk management dialogue that must occur between cyberinsurers, brokers, and policyholders regarding the need for adequate cyberliability insurance protection.

The Litigious Aftermath of *The Interview* Attack

To date, nine class action lawsuits have been filed against Sony in California state and federal courts. See *Dukow v. Sony Pictures Entm't*, No. BC566884 (L.A. Cnty. Superior Ct.); *Doe v. Sony Pictures Entm't*, No. BC567358 (L.A. Cnty. Superior Ct.); *Corona v. Sony Pictures Entm't*, No. 2:14-cv-9600-RGK-SH (C.D. Cal.) (the plaintiffs in the seven federal court actions have moved to consolidate the lawsuits—

■ Matthew S. Foy is an insurance partner in the San Francisco, California, office of Gordon & Rees LLP and serves as the national practice group leader for the firm's property and casualty insurance practice. Mr. Foy represents insurers nationally in connection with coverage litigation and advice involving primary and excess liability policies with an emphasis on complex Coverage B, mass tort, professional liability, and environmental matters.



He also currently serves as vice chair of DRI's Insurance Law Committee. Jonathan L. Schwartz is a partner in the Global Insurance Services group of Goldberg Segalla. He resides in the Chicago, Illinois, office and concentrates his practice on insurance coverage litigation and counseling, including primary and excess commercial general liability, cyberliability, professional liability/E&O, transportation, and D&O liability insurance policies. Jonathan is the chair of the DRI Insurance Law Committee's Advertising Injury and Personal Injury Subcommittee and a longtime member of the committee's Steering Committee. Collin Willmott of Goldberg Segalla LLP assisted in the preparation of this article. We wish to thank him for his invaluable efforts.

that motion remains under consideration). These suits collectively allege that Sony failed to remedy the known defects and vulnerabilities in its security systems, failed to implement adequate and effective information security policies and procedures in accordance with industry standards and best practices, and unreasonably delayed in notifying the affected individuals of the breach. Notably, the putative class representatives rely on Sony's prior experience with cyberattacks, including the April 2011 attack in which hackers gained access to the Sony PlayStation Network and stole PII of more than 100 million customers.

Cyber-Threat Proliferation

According to the FBI, hacking at small businesses "is a prolific problem." See Geoffrey A. Fowler and Ben Worthen, "Hackers Shift Attacks to Small Firms," *Wall Street Journal*, July 21, 2011. The Hartford found in 2012 that one-third of cyberattacks occurred at businesses with fewer than 100 employees. Symantec also found that 40 percent of attack victims are small- and medium-sized businesses. According to the Ponemon Institute, a company with less than 10,000 records is more likely to be hacked than a company with more than 100,000 records. See Mary Thompson, "Why Cyber-Insurance Will Be the Next Big Thing," *CNBC*, Jul. 1, 2014 (quoting Robert Parisi of Marsh USA, "Hackers and cybercriminals are very opportunistic[.] If they can get 100 records or credit cards from the local dry cleaners they'll do it.").

And, this problem is about to get worse for businesses large and small. "The risk of data breach will increase significantly as business information is shifted to cloud computing services... and mobile devices are used more to store and transmit confidential data." See Jonathan L. Schwartz, "If a Tree Falls in a Forest and No One Is Around to Hear It, Does It Make a Sound? Whether Allowing Unauthorized Access to or a Failure to Protect Personally Identifiable Information Constitutes 'Personal and Advertising Injury'?", *Covered Events*, August 2012.

A data breach without adequate insurance can devastate a business. Accord-

ing to the Ponemon Institute, the average total cost of a breach in the United States is now \$5.9 million. In addition to multiple civil lawsuits, a business may face regulatory proceedings and the prospect of fines of hundreds of thousands or millions of dollars.

■

The Hartford found in 2012
that one-third of cyberattacks
occurred at businesses with
fewer than 100 employees.

■

Data Breach Exposures Should Not Be Covered Under Commercial General Liability Policies

The insurance industry never contemplated that traditional CGL policies covering Bodily Injury and Property Damage Liability (Coverage A) and Personal and Advertising Injury Liability (Coverage B) would be called upon to insure against data breach exposures faced by companies like Sony. Nonetheless, insureds (and in particular those without any cyberliability insurance whatsoever, or inadequate cyberliability coverage) have and can be expected to continue to turn to their CGL insurers for coverage. There are numerous reasons why the exposures typically presented by data breach litigation are not covered or even potentially covered under CGL policies, as courts across the country have begun to recognize.

Coverage A

In traditional data breach cases, most policyholders do not even endeavor to argue that the resulting exposures are covered under Coverage A – Bodily Injury and Property Damage Liability. Nonetheless, issues under Coverage A can and sometimes do arise.

While it is rare for a data breach plaintiff to assert a claim against the insured for traditional "bodily injury" involving a purely physical manifestation of injury, claims

for emotional distress or mental anguish are at least conceivable. The prevailing view is that claims for emotional distress or mental anguish, unaccompanied by physical injury, do not constitute "bodily injury," as that term is typically defined in CGL policy forms. See, e.g., *Aim Ins. Co. v. Culcasi*, 229 Cal. App. 3d 209, 220, 280 Cal. Rptr. 766 (1991); *Trinity Universal Ins. Co. v. Cowan*, 945 S.W.2d 819, 823 (Tex. 1997). Some courts, however, have relied on perceived ambiguities in the definition of "bodily injury" to conclude it can encompass emotional distress claims. See, e.g., *Lavanant v. Gen. Accident Ins. Co.*, 79 N.Y.2d 623, 630, 79 N.Y.2d 623 (1992) (the terms "sickness" and "disease" in the definition of "bodily injury" may be viewed by the average reader to include mental as well as physical sickness). In cases where emotional distress claims are asserted, consideration must also be given to whether the policy includes a non-standard "bodily injury" definition, which may encompass emotional distress, either alone or when accompanied by physical injury.

Turning to "property damage" coverage, rare will be the case where a data breach plaintiff asserts a claim against the insured that encompasses "physical injury to tangible property" or "loss of use of tangible property that has not been physically injured." While data breach incidents can result in the loss of electronic data, such data is by its very nature not "tangible" property; without physical injury to or loss of use of "tangible" property, the traditional definition of "property damage" is simply not implicated. See, e.g., *Warner v. Fire Ins. Exch.*, 230 Cal. App. 3d 1029, 1035, 281 Cal. Rptr. 635 (1991) (the term "tangible property" is understood in its "plain and ordinary" sense to mean "property (as real estate) having physical substance apparent to the senses"); *Cincinnati Ins. Co. v. Prof'l Data Servs., Inc.*, 2003 U.S. Dist. LEXIS 15859, *21 (D. Kan. 2003) (loss of use of software and data is not "property damage" because neither has "any physical substance [or] is perceptible to the senses"); *Am. Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89, 96 (4th Cir. 2003) (Virginia law) (same); see also Schwartz, *supra*.

To clarify the intent and common sense interpretation that claims involving loss of

electronic data are not covered, the 2001 revision to the ISO CGL form amended the definition of "property damage" to specifically state that "electronic data is not tangible property" and, further, that "electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment." See ISO form CG 00 01 12 07. Additionally, and as part of the 2004 CGL revision, ISO introduced exclusion "p" (the Electronic Data Exclusion) which broadly eliminates coverage 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." See ISO form CG 00 01 12 04.

Policyholders that seek CGL coverage to help defray their data breach exposures are not without options. As part of its 2004 revision, ISO introduced an Electronic Data Liability Coverage Form that provides claims-made coverage, subject to a number of exclusions, for an "electronic data incident" that causes "loss of electronic data." See ISO form CG 00 65 12 04. The term "electronic data incident" is defined as "an accident, or a negligent act, error or omission... which results in loss of electronic data." "Loss of electronic data" is defined, in turn, as "damage to, loss of, loss of use of, corruption of, inability to access, or inability to properly manipulate, 'electronic data.'"

Coverage B

Most of the coverage disputes resulting from data breach incidents have focused on Coverage B – Personal and Advertising Injury Liability. The insuring agreement under Coverage B typically provides coverage for "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 your business[.]" The "offense" most frequently targeted by policyholders in connection with data breach exposures is the offense for "oral or written publication, in any manner, of material that vio-

lates a person's right of privacy," referred to herein as the "Right of Privacy" offense.

A preliminary consideration when addressing policyholder tenders of data breach lawsuits is whether the underlying claimants have asserted a common law claim for "invasion of privacy." Often they do not, electing instead to assert claims

■

The prevailing view is
that claims for emotional
distress or mental anguish,
unaccompanied by physical
injury, do not constitute
"bodily injury," as that
term is typically defined
in CGL policy forms.

■

for negligence, breach of contract, or violation of any number of statutes governing electronically stored information, medical records, or business acts and practices. This is relevant because Coverage B offenses should be interpreted by reference to the common law torts which they embody, e.g., invasion of privacy. See *Fibreboard Corp. v. Hartford Accident & Indem. Co.*, 16 Cal. App. 4th 492, 511, 20 Cal. Rptr. 2d 376 (1993) ("The listed offenses... are not separately defined in the policies. We thus give them meaning by reference to their common law elements").

Most courts agree that an insurer's duty to defend is determined by the facts alleged in the complaint, rather than the labels of the causes of action asserted. See, e.g., *Travelers Ins. Cos. v. P.C. Quote, Inc.*, 211 Ill. App. 3d 719, 729, 570 N.E.2d 614 (1991); *Barnett v. Fireman's Fund Ins. Co.*, 90 Cal. App. 4th 500, 510, 108 Cal. Rptr. 2d 657 (2001). As a result, the absence of a specific "invasion of privacy" cause of action is not, by itself, coverage determinative. But just what a claimant must allege to raise

a potential for coverage under any of the Coverage B offenses, including the Right of Privacy offense, continues to be an issue that is litigated in a variety of contexts. See, e.g., *Liberty Bank of Montana v. Travelers Indem. Co.*, 870 F.2d 1504, 1508 (9th Cir. 1989) (Montana law) (no duty to defend under Coverage B where the elements of defamation were not alleged).

A separate issue relates to the requirement under the Right of Privacy offense that there be an "oral or written publication." Courts across the country have struggled with interpretation of the "publication" requirement. Many courts hold that "publication" requires widespread dissemination of private information to the public at large. See, e.g., *Penzer v. Transp. Ins. Co.*, 29 So. 3d 1000, 1005–1006 (Fla. 2010); *TIG Ins. Co. v. Dallas Basketball, Ltd.*, 129 S.W.3d 232, 238 (Tex. App. 2004). Other courts have found a potentially covered "publication" to exist where there is a less-than-public dissemination of information. See, e.g., *LensCrafters, Inc. v. Liberty Mut. Fire Ins. Co.*, 2005 U.S. Dist. LEXIS 47185, *35 (N.D. Cal. 2005); *Pietras v. Sentry Ins. Co.*, 2007 U.S. Dist. LEXIS 16015, *10 (N.D. Ill. 2007).

Regardless of how any particular court interprets the "publication" requirement under the Right of Privacy offense, that requirement should not be satisfied in the context of underlying data breach claims like those faced by Sony. Plaintiffs in those cases typically file suit based on the insured defendant's alleged failure to safeguard data, thus permitting third party criminals to access PII for any number of illicit purposes. The resulting exposure is not based on, and in fact has nothing to do with, the insured's own "oral or written publication" of any material, as is required for Right of Privacy coverage to apply. While data breach claimants sometimes allege that the insured itself "divulged" or otherwise "disclosed" the accessed information, such conclusory allegations are always at odds with the true nature of the facts alleged and the gravamen of the theories advanced; thus, they should have no bearing on the duty to defend.

While the compromise of PII is inherent in most data breaches, lack of "publication" is also a coverage defense where the inci-

dent has not resulted in any alleged harm. Particularly in the class action context, it is not uncommon to find data breach claimants allege that they have been placed at greater risk of identity theft or other possible, future harm. Even under the broadest interpretation, the “publication” requirement under the Right of Privacy offense should not be satisfied in the absence of allegations or evidence that the claimants’ personal information has been accessed or otherwise resulted in some existing, identifiable harm.

That was the conclusion reached by the Connecticut Appellate Court in *Recall Total Information Management v. Federal Insurance Co.*, 147 Conn. App. 450, 147 Conn. App. 450 (2014). In that case, Recall contracted with IBM to store electronic data, which included the personal information of more than 500,000 current and former employees. Recall also contracted with a company to transport the IBM data tapes. While in transit, the tapes fell off the back of a truck, were taken by unknown persons, and never recovered. IBM incurred over \$6 million in mitigation costs, including sending notifications to affected persons and providing credit monitoring services. IBM issued a demand to Recall. Following a settlement, Recall initiated coverage litigation against the transport company’s liability insurers. Recall argued that the personal information stored on the data tapes had been “published” to a thief or unknown persons, triggering Coverage B under the transport company’s liability policies. The Connecticut Appellate Court disagreed, concluding that the mere exposure of personal information does not constitute a “publication” without evidence the information was actually accessed or resulted in injury to the IBM employees. *Id.* at 463–464.

Consistent with the foregoing, data breach claims should not be covered under the Right of Privacy offense for an additional, significant reason—the insured’s liability in those cases is not based on its own intentional conduct. This issue was and continues to be litigated in the widely publicized coverage litigation resulting from the 2011 data breach of Sony’s online gaming networks. In response to Sony’s tender of dozens of class action law-

suits resulting from that breach, its insurers declined coverage, and Zurich filed a declaratory relief action in New York. See *Zurich Am. Ins. Co. v. Sony Corp. of Am., et al.*, Supreme Court of the State of New York, County of New York, Case No. 651982/2011.

On February 21, 2014, Judge Jeffrey Oing ruled on the parties’ cross-motions for

■

Enforcing CGL policies
as written and without
judicial expansion of the
coverage provided will allow
the insurance market to
function properly through
the setting of appropriate
premiums that take into
account the specific types
of exposures the policies
were designed to cover.

■

summary judgment and held that Sony’s insurers owed no duty to defend under the Right of Privacy offense. Judge Oing recognized that in contrast to Coverage A (which provides “occurrence” based coverage for “bodily injury” or “property damage” resulting from the insured’s negligent conduct), Coverage B provides “offense” based coverage for exposures resulting from the insured’s affirmative, intentional acts. Like all traditional data breach suits, Sony’s liability was premised on its negligent failure to safeguard against the attack on its online gaming networks. The only affirmative, intentional conduct at issue was perpetrated by third party criminals. Judge Oing ruled that in the absence of any “oral or written publication” of material by Sony that violated the privacy rights of the claimants, the Right of Privacy offense

was not implicated, and no duty to defend was owed.

In so holding, Judge Oing relied on decisions from across the country that have correctly recognized that the enumerated offenses under Coverage B afford coverage that is limited to protecting against the purposeful and intentional acts committed by the insured or its agents, not by non-insured third parties. See, e.g., *Cnty. of Columbia v. Cont’l Ins. Co.*, 595 N.Y.S.2d 988, 189 A.D.2d 391 (3d Dept. 1993), *aff’d*, 83 N.Y.2d 618, 627–628 (1994) (personal injury offenses intended to cover only purposeful acts undertaken by the insured or its agents); *Butts v. Royal Vendors, Inc.*, 202 W. Va. 448, 454, 504 S.E.2d 911 (1998) (offense for “oral or written publication” “was not written to cover publication by a third-party”); *Gregory v. Tennessee Gas Pipeline Co.*, 948 F.2d 203, 209 (5th Cir. 1991) (Louisiana law) (each of the Coverage B offenses “requires active, intentional conduct by the insured”).

Judge Oing rejected Sony’s argument that there was no express requirement under Coverage B that the insured, itself, had to commit the offense for coverage to apply as inconsistent with the plain language of the policy interpreted as a whole. Judge Oing also rejected Sony’s argument that the fact an “oral or written publication” of material under the Right of Privacy offense can occur “in any manner” expanded coverage to third party publications. “[T]he phrase ‘in any manner’ merely expands the categories of publication (such as e-mail, handwritten letters, and, perhaps, “blast-faxes”) covered by the Policy.” *Creative Hospitality Ventures, Inc. v. U.S. Liab. Ins. Co.*, 444 Fed. Appx. 370, 376 (11th Cir. 2011). That phrase has no effect on the requirement that the insured’s liability result from its own publication of material in the first instance.

On April 9, 2014, Sony appealed from Judge Oing’s ruling. The parties’ briefing is presently before the Appellate Division of the Supreme Court of the State of New York. Policyholders and the insurance industry alike are closely monitoring this appeal and the Appellate Division’s treatment of the core legal arguments. Public policy considerations are also expected to play a role in the Appellate Division’s con-

sideration of the issues, noting that Sony and an increasing number of insureds are purchasing cyber policies to cover the very exposures at issue.

Because data breach exposures do not plainly fit within the coverage provided by CGL policies, and were never intended to, industry experts uniformly recommend that companies look to specialty cyber insurance products for protection. See, e.g., Cybersecurity report, National Association of Insurance Commissioners & The Center for Insurance Policy and Research, http://www.naic.org/cipr_topics/topic_cyber_risk.htm (“[M]ost standard commercial lines policies do not cover many of the cyber risks mentioned above. To cover these unique cyber risks through insurance requires the purchase of a special cyber liability policy.”); 1 Internet Law and Practice §2:49 (“[T]he insurance industry has developed new products aimed specifically at e-commerce and other cyber liability.”) Enforcing CGL policies as written and without judicial expansion of the coverage provided will allow the insurance market to function properly through the setting of appropriate premiums that take into account the specific types of exposures the policies were designed to cover.

As a response to policyholder efforts to secure coverage under the Right of Privacy offense for an ever-expanding range of exposures (including data breach exposures) that the insurance industry never intended to be covered, ISO has introduced broad privacy-related endorsements which clarify that intent and eliminate any arguments for coverage. In 2013, ISO came out with the “Amendment of Personal and Advertising Injury Definition” endorsement, which provides that the offense for “[o]ral or written publication, in any manner, of material that violates a person’s right of privacy” is simply eliminated from the definition of “personal and advertising injury.” See ISO Form CG 24 13 04 13. Additionally, in 2014, ISO introduced an “Exclusion – Access or Disclosure of Confidential or Personal Information and Data Related Liability,” which makes clear that Coverage B does not apply to a wide range of damages frequently claimed in data breach litigation “arising out of any access to or disclosure of any person’s or organiza-

tion’s confidential or personal information, including... financial information, credit card information, health information or any other type of nonpublic information.” See ISO Form CG 21 06 05 14.

Following Judge Oing’s ruling in the Sony coverage litigation, and the introduction of the ISO endorsements clarifying

■

Hence, courts examining these exclusions under circumstances like those involved in the Sony breach or like breaches in the future can be expected to turn to established case law issued in connection with physical attacks

■

the insurance industry’s intent that data breach exposures are not covered under CGL policies, policyholders have already begun to, and will continue to, flock to the specialty cyberinsurance marketplace. And rightly so, as cyberliability insurance policies are specifically designed to cover these data breach exposures, as discussed below. See Michael T. Glascott and Aaron J. Aisen, “The Emperor’s New Clothes and Cyber Insurance,” *FDCC Quarterly*, Spring 2013, p. 201 (“Cyber insurance products were also developed to provide coverage for the gap inherent in Commercial General Liability (CGL) policies for damage which is not tangible, along with the peripheral costs caused by cyber security breaches.”).

The Added Wrinkle of Cyberattacks by State Actors Raises Additional Insurance Issues

The fact that *The Interview* Attack was allegedly committed by North Korea, a hostile government, against Sony, a private

corporation, could have a profound impact on the availability of Sony’s insurance coverage. A standard ISO War exclusion (CG 00 01 12 07, Exclusion i.) states that coverage does not apply to war, undeclared or civil, or “warlike action by a military force, including action in hindering or defending against an actual or expected attack, by any government, sovereign or other authority using military personnel or other agents...” Incidents involving computer hacks do not fall under the traditional concept of “war.” However, what constitutes “warlike action” is an evolving concept. An increasing number of military experts consider cyberspace to be the “battlefield of the future.” Most militarily advanced nations, including the United States and Russia, have robust cyberwarfare units. Thus, in the context of a cyberattack, “War” exclusions require consideration.

Whether *The Interview* Attack against Sony might be considered “warlike action” is yet to be determined. The United States government has been reluctant to characterize *The Interview* Attack as “terrorism” or an “act of war.” President Obama instead labeled the incident as “cyber-vandalism.” By contrast, North Korean spokesmen have hyperbolically characterized *The Interview* as “undisguised terrorism” and an “act of war.”

There are no published decisions interpreting the War exclusion in connection with a cyberattack. Hence, courts examining these exclusions under circumstances like those involved in the Sony breach or like breaches in the future can be expected to turn to established case law issued in connection with physical attacks. Compare *Cedar & Washington Associates, LLC v. Port Authority of N.Y. & N.J. (In re September 11 Litigation)*, 751 F.3d 86 (2d Cir. 2014) (deciding that 9/11 was an “act of war” even though it was not perpetrated by a state or government), with *Pan Am. World Airways Inc. v. Aetna Cas. & Surety Co.*, 505 F.2d 989 (2d Cir. 1974) (holding that coverage for the loss of the aircraft resulting from a hijacking by the Popular Front for the Liberation of Palestine was not barred by the War exclusion because the incident was not caused by a war waged between two states or state-like entities). Based on these cases, there

is clearly room for debate over what may be considered “warlike action.”

The Cyberliability Insurance Imperative for Businesses Large and Small

Data breaches are no longer a question of if, but rather of when. See Kristi Singleton and Scott Godes, “Top Ten Tips for Companies Buying Cyber Security Insurance Coverage,” *Association of Corporate Counsel*, Dec. 20, 2012 (“Unfortunately, no wall is unbreachable, and no security system impenetrable.”); Robert S. Mueller, III, Director, Federal Bureau of Investigation, RSA Cyber Security Conference in San Francisco, Mar. 1, 2012, available at <http://www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies> (last visited Feb. 17, 2015) (“there are only two types of companies: those that have been hacked and those that will be”). One leading commentator on cybercoverage remarked, “The headlines confirm the reality: cyber attacks are on the rise with unprecedented frequency, sophistication, and scale. They are pervasive across industries and geographical boundaries and present ‘an ever-increasing threat.’” Roberta D. Anderson, “Viruses, Trojans, and Spyware, Oh My! The Yellow Brick Road to Coverage in the Land of Internet Oz,” *American Bar Association Tort Trial & Insurance Practice Law Journal*, 49 *Tort & Ins. L.J.* 529, Winter 2014 (describing cybersecurity breaches as “ubiquitous” and acknowledging the existence of one category: “companies that have been hacked and will be hacked again”).

Even with the most advanced cyberdefenses, the largest of companies are still at risk for cyberattacks. According to Sony Entertainment’s CEO, Michael Lynton, the malware used in *The Interview* Attack was so sophisticated that it would have overcome the cyberdefenses of 90 percent of U.S. businesses. That figure likely is much higher for small and mid-size businesses, whose cyberdefenses are not nearly as robust as those of Fortune 50 companies. And, that is highly problematic because on average, according to the Ponemon Institute, U.S. companies can expect to pay an average of \$201 per compromised record. That includes costs for forensics inves-

tigation, providing credit monitoring to affected individuals, crisis management services, defense costs for lawsuits and regulatory proceedings, damage awards resulting from the lawsuits, and regulatory fines.

Given the ever-present and increasing risk of data breach exposure facing com-

■

As the cyberinsurance market has evolved, the product offerings are becoming more similar with functionally identical coverages, definitions, and exclusions (even if the products have different names and use different wordings).

■

panies domestic and abroad, cyberliability insurance is “the last line of defense” for businesses with an online presence or that store electronically PII. See Peter K. Rosen, Bob Steinberg, Margrethe K. Kearney, Martha L. O’Connor, and Neil A. Rubin, “Cyber Insurance: A Last Line of Defense When Technology Fails,” *Latham & Watkins Client Alert White Paper*, Apr. 15, 2014 (“[T]he deck is stacked against the defender, because the cyber attacker only needs to find one vulnerability—often the humans rather than the computer systems—and exploit it, while the security vendor must try to anticipate every attack and block them all.”). Businesses are increasingly recognizing that reality. It is expected that businesses will spend at least \$2 billion in cyberinsurance premiums in 2014, an increase of 67 percent from 2013. See Cory Bennett, “Demand for Cyber Insurance Skyrockets,” *The Hill*, Jan. 15, 2015; Abha

Bhattarai, “Cyber-insurance Becomes Popular Among Smaller, Mid-Size Businesses,” *Washington Post*, Dec. 19, 2014. And that number will increase every time there is another mega-breach, as cyberliability “advertises itself each time you hear about another major cyber-breach.” See Bhattarai, *supra*; see also Bennett, *supra* (quoting a Marsh executive, “Every major breach gets companies off the sidelines and moves them towards purchasing.”). Surveys by Marsh, however, indicate that only 30 percent of small and midsize companies carry cyberinsurance.

Smaller and midsize companies will hopefully improve that number dramatically. That is because cyberinsurance is everywhere now, as it is believed to be “the new frontier for insurance companies looking to grow.” See Luciana Lopez, “Risk Modelers Working on Tools for Gauging Cyber Attack Risk,” *Insurance Journal*, Dec. 23, 2014; see also Noah Buhayar, Sarah Jones, and Zachary Tracer, “P/C Insurers Rush to Meet Rising Demand for Cyber Insurance,” *Insurance Journal*, Oct. 9, 2014 (“[Insurers] now see cyber insurance as a once-in-a-generation opportunity that is set for growth.”). Approximately 50 insurers offer cybersecurity insurance to U.S. companies. See Bhattarai, *supra*. As additional evidence that cyberinsurance is mainstream, the National Association of Insurance Commissioners recently announced the formation of a new cybersecurity task force and affirmed its commitment to regulating cyberinsurance.

One of the reasons smaller and midsize companies may be shying away from cyberinsurance is that the procurement and application process can be daunting. But perception does not quite match reality. As will be discussed throughout the rest of this section, purchasing cyberinsurance requires an open, high-level dialogue between insurance carriers and applicants. We will describe the available offerings in the cyberliability insurance market and the areas of peak concern for insurance carriers and applicants.

The Cyberinsurance Market Is No Longer the “Wild West”

A common refrain used to describe cyberinsurance policies is that the terms vary

dramatically. See, e.g., Richard S. Betterley, *Cyber/Privacy Insurance Market Survey*, Betterley Rep., June 2013, available at: <http://www.irmi.com/products/store/betterley-report.aspx> (last visited Feb. 17, 2015). While there is no uniform or standard cyberliability insurance policy yet, and that refrain may have been true at the beginning of this decade, the refrain is no longer accurate. As the cyberinsurance market has evolved, the product offerings are becoming more similar with functionally identical coverages, definitions, and exclusions (even if the products have different names and use different wordings). Our review of more than a dozen specimen cyberliability policies from leading insurers confirms that reality. Those include: Liberty Surplus Insurance Corporation's Data Breach and Network Protection Insurance policy (LSI DI P001 (Ed. 06 13)), OneBeacon Professional Insurance's Network Security and Privacy Liability (NPF-51001-11-12), IronShore Specialty Insurance Company's Enterprise PrivaProtector 9.0 (PSN.COV.001 (01.12)), AIG's CyberEdge PC (4/25/2014), AXIS Pro's Privasure Breach Response Insurance Policy (PBR-0300 (05-11)), ACE's Privacy & Network Liability Insurance Policy (PF-26999 (05/09)), Travelers' Cyberrisk Policy (CYB-3001 Ed. 07-10), Philadelphia Indemnity Insurance Company's Cyber Security Liability Coverage Form (PI-CYB-001 (08/12)), Zurich's Security and Privacy Protection Policy (U-SPR-1000-C CW (02/14)), Beazley's Information Security & Privacy Insurance with Electronic Media Liability Coverage (F00106 052011 ed.), and Chubb's Cybersecurity policy (14-02 14874 (02/2009)). Please know that the operative cyberliability forms change frequently. We thus encourage readers to inquire of their broker whether the forms we have reviewed are still the most current.

While cyberliability insurance policy forms are becoming more standardized, the market is highly competitive, and the products can be highly negotiable and are often customized. See Anderson, *supra*. Policyholders are, in all likelihood, in a better negotiating position now with respect to cyberinsurance policies than they will ever be again. This is especially true for small and mid-size businesses, whose losses from a cyberattack are considered less severe

than those experienced by large retailers such as Target and Home Depot, as insurers are increasingly focusing on them as profitable segments of the market. See Andrea Rumbaugh, "Cyberinsurance a Hot Topic After Data Breaches," *Houston Chronicle*, Jan. 22, 2015.

■

Before entering into negotiations, policyholders should be well aware of their other insurance coverages and indemnity agreements, and should do their utmost to avoid purchasing overlapping coverages or leaving significant gaps in coverage.

■

Available Cyberliability Coverages

This section focuses on cyberliability coverage and the other attendant coverages necessary to respond to a data breach affecting third parties. There are other first- and third-party coverages available for purchase in connection with a cyberinsurance policy, including personal injury liability coverage (e.g., intellectual property infringement, defamation, invasion of privacy, etc.), business interruption coverage, reputation coverage, and data asset coverage (i.e., restoring the insured's own systems following an attack). However, those coverages merit their own separate discussion, apart from this article, which focuses on liability claims in the aftermath of a data breach.

Cyberinsurance coverages are sold à la carte, on a claims-made or claims-made-and-reported basis. First, there is data breach liability coverage, which pro-

vides defense and indemnity for the insured against lawsuits resulting from a data breach. Second, there is regulatory proceeding coverage, which also provides defense and/or indemnity for the insured against governmental investigations resulting from a data breach. Third, there is response cost coverage, which provides for forensic investigation, counsel regarding notification requirements, credit monitoring and identity restoration services, crisis management/public relations services, and call centers. Typically, all of these coverages are subject to a general aggregate, and sub-limits for many of the coverages are common.

Risk Control and Negotiation: Everybody Should Be Prepared to Disclose and Assess

The biggest challenge involved in the selling and buying of cyberliability insurance is the lack of actuarial or empirical data on cyberattacks, which makes it difficult to make premium calculations with precision. This challenge is intensified by the reality that information about previous attacks is not too helpful for insurers because hackers are always increasing in sophistication. According to Graeme Newman, a director at CFC Underwriting, "Statistics from five years ago are almost irrelevant today." See Nicole Perlroth and Elizabeth A. Harris, "Cyberattack Insurance a Challenge for Business," *New York Times*, Jun. 9, 2014.

Insurers thus must rely on qualitative assessments of the applicant's data security measures. This demands a highly sophisticated risk control program and a concerted effort by insurers to hire or retain enough knowledgeable and experienced individuals to rigorously evaluate the very specific capabilities and vulnerabilities of an applicant. It also requires an understanding by applicants that cybersecurity is no longer just an IT or a risk management problem. It is an enterprise-wide concern that requires the involvement of the board of directors and/or members of the C-suite. At a minimum, a company's chief information security officer or chief information officer, who should have the best awareness of the company's cyber-risk, must be directly involved.

The sale and purchase of a cyberliability insurance policy requires a dialogue about risk. From the policyholder's perspective, it needs to be certain that it is getting the coverage the business needs should it be subjected to a cyberattack. From the insurer's perspective, it needs to be certain that it is charging an adequate premium to account for the policyholder's particular vulnerability to an attack.

In surveying the specimen policies and applications, it is apparent that the following are the key issues that need to be discussed in any dialogue about cyberinsurance. Yet, the overarching question that should pervade the dialogue is, what are the applicant's particular cyber-risks?

Policyholder Top 10 Considerations

In negotiating the terms of the cyberliability insurance policy, the following are the top 10 cyber-specific considerations for an applicant. They are not recognized standards or best practices—merely suggestions. Also, they are not in a particular order of importance. Before entering into negotiations, policyholders should be well aware of their other insurance coverages and indemnity agreements, and should do their utmost to avoid purchasing overlapping coverages or leaving significant gaps in coverage.

1. Know Your Limits. One of the most important considerations for a policyholder in purchasing cyberliability insurance coverage is its particular exposure. Having an understanding of what exposure is presented by its maintenance of confidential information, under a worst-case scenario, will help a policyholder to purchase adequate insurance. Attacks can cripple a small or mid-size company, so being underinsured defeats the purpose of buying cyberliability insurance. Thus, the policyholder must be keenly aware of the insurance limits it needs to be protected from the aftermath of an attack. In particular, a policyholder should consider what aggregate limit and sublimit for attendant coverages are necessary. The policyholder also must decide whether to purchase an eroding or wasting limits policy, *i.e.*, one where defense costs are within the limits of the policy. Notably, most carriers are reluctant to offer more than \$10 million in cov-

erage, so building a tower of cyberliability coverage may be essential.

2. Retroactive Date/Knowledge Date/Continuous Coverage. There are already reports that hackers spent more than two months mapping Sony's computer systems before committing *The Interview* Attack. That is not unusual because data breaches can go

■

Taken together, these considerations seek to identify the strengths and weaknesses of the applicant's cybersecurity defenses, as well as the applicant's attitude and experience with cybersecurity matters.

■

undetected for months or years. See Verizon, Data Breach Investigations Report (2014). Given the claims-made nature of cyberliability policies, they will necessarily require that the wrongful act or injury giving rise to the subject claim occur after a negotiated retroactive date. Policyholders should be mindful of securing a retroactive date that will cover breaches that took place well prior to the inception date of the policy. Further, many cyberliability insurance policies allow for a wrongful act to have occurred prior to the inception date of the first policy in a series of policies continuously issued by the insurer. That provision may be essential. Also, some cyberliability insurance forms utilize a "knowledge date" and require that no executive, director, or officer of the applicant knew or reasonably could have known of a wrongful act or injury that might give rise to the claim. As with the retroactive date, policyholders should be mindful of securing a "knowledge date" that will cover breaches

that took place prior to the inception date of the policy.

3. Flexibility in Attendant Coverages. Cyberinsurers typically sell attendant coverages for the myriad types of services needed to effectively respond to a data breach. Most carriers have an approved panel of firms or service providers and may seek to compel the policyholder to use the approved list. There is great value in having a team of forensic investigation firms, customer notification services, credit monitoring and identity restoration services, call centers, public relations professionals, and post-breach legal counsel in place in advance of any breach. It appears that some insurers may be willing to accommodate a policyholder's preference for certain vendors with which it has experience or a prior relationship. Yet, the insurer will generally pay the policyholder's chosen vendors only at the rate charged by the insurer's approved vendors.

4. Claims by Employees. All of the recently filed lawsuits faced by Sony are brought by current or former employees' whose confidential information was breached and released. As a lesson to other companies, be sure that any "insured versus insured" exclusion in a cyberliability policy contains an exception for claims brought by employees of the company.

5. Property Damage Caused by the Cyberattack. Policyholders should give due consideration to whether they need to purchase coverage for "property damage" resulting from an attack. There have been reports of data breach incidents causing physical damage to a Turkish pipeline, Iran's nuclear centrifuges, and a German steel factory. Notably, the CGL data breach exclusion discussed above contains, for purposes of CGL Coverage A, a "bodily injury" exception, but not a "property damage" exception.

6. Severability Provisions. There has been some speculation that a current or former Sony employee was involved in or contributed to *The Interview* Attack. Many cyberliability policies contain an exclusion for claims resulting from dishonest, deceptive, or illegal conduct by the insured. They also typically contain an exception or severability provision that precludes the imputing of an insured's conduct to the entire company,

as long as the offending person was not a director, officer, principal, or other like person. Having a broad exception to this wrongful conduct exclusion can be critically important, especially given the possibility that a rogue employee was involved or participated in the breach.

7. Exceptions to War/Terrorism Exclusions. Many cyberliability policies contain War or Terrorism exclusions akin to those found in CGL policies. Some expressly cover or except cyberterrorism from these exclusions. It makes a lot of sense to negotiate for that coverage, especially in light of the circumstances of *The Interview* Attack on Sony allegedly perpetrated by North Korea. Notably, insurers appear willing to offer a cyberterrorism exception to the War exclusion. See Jeff Sistrunk, "Sony Hack Shows Need for Cyber Coverage on Many Fronts," *Law360*, Jan. 9, 2015.

8. Other Parties in Control of Your Data. Policyholders should be highly attuned to whether the cyberliability insurance policy covers misconduct by a vendor, subcontractor, or other independent contractor whom they retained or with whom they have contracted. As website, network, data processing, and data storage functions, among others, are outsourced to third-party vendors, it is essential that policyholders secure coverage for a wrongful act committed by the third-party which causes a loss of data for which claimants will allege the policyholder is legally responsible.

9. Coverage for Payment Card Industry Liability. Data breaches involving customer credit card numbers can raise the added wrinkle of credit and debit card companies pursuing relief from the attacked company. Some cyberliability insurance policies cover fines or penalties levied by the credit card association. That coverage may very well prove invaluable.

10. Stringent Notice Requirements. While most cyberliability insurance policies require notice of a claim be provided to an insurer "as soon as practicable," *i.e.*, within a reasonable time, notice of an attack or breach incident may not be as flexible for policyholders. Many of the policies have an additional notice requirement that notice of an attack or breach be provided within 30, 60, or 90 days after the company becomes aware of it. That may not

ultimately become an issue, as most companies are very diligent about notifying their insurers of a major attack. However, it may be a different story for attacks without apparent damage or loss of control of data. Since the failure to provide timely notice of the incident can prove fatal and result in a loss of coverage for the policyholder, pol-

■

It is presently a soft market,
and policyholders have the
ability to fully customize their
policy package in order to
provide a robust "last line of
defense" to a cyberattack.

■

icyholders should be acutely aware of all notice and timing requirements in their cyberinsurance policies.

Insurer Top 10 Considerations

The following are the top 10 cyber-specific considerations for an insurer in evaluating the applicant's risk. Again these are merely suggestions—not standards—and are not in a particular order of importance.

1. What kind of target is the applicant? Does the applicant store valuable PII, such as credit card and bank account numbers, social security numbers, medical records, and the like? Similarly, does the applicant allow online purchases or bill payment? Also, does the applicant store other businesses' proprietary information, including customer and employee information and intellectual property and trade secrets? The amount and nature of information stored by the applicant could be directly related to their risk of a cyberattack.

2. Industry and Geography. Underwriters need to be attuned to the particular cyber-risks attendant to the applicant's industry. Retailers, for instance, tend to store a lot of customer financial information. Additionally, understanding the geographic spread of the applicant's business operations is

crucial. Data security laws vary from state to state, and the more states an applicant does business in, the more states' laws will be implicated for purposes of notifying customers and employees, whose confidential information/data has been breached.

3. Leadership Structure. Underwriters must understand how seriously the applicant is taking cybersecurity and whether it has individuals in place to assess and respond to cyber-threats. That includes whether the applicant has in place a Chief Information Security Officer (or similar executive) and an Incident Response Plan and Team.

4. Cybersecurity Priorities. Underwriters should similarly understand how the applicant prioritizes its resources with respect to prevention of attacks versus detection of attacks and threats versus responses to attacks. This also requires consideration of the cybersecurity policies and protocols the applicant has in place, including with respect to mobile devices, laptops, removable media/USB devices, and "bring your own device" plans. Plus, the underwriters should endeavor to learn the company's strategy for updating and upgrading its cybersecurity measures.

5. Industry Frameworks. In February 2014, the National Institute of Standards and Technology announced a new framework for cybersecurity infrastructure. It provides standards and practices with respect to cyber-risk. Whether the applicant has adopted the NIST Cyber Framework or a comparable cybersecurity standard may signify the applicant's commitment to overall good cybersecurity practices.

6. Technical Vulnerabilities. Underwriters must be aware of applicant's cyberdefenses and weaknesses in its data security systems. Most important, does the applicant have regular cybersecurity audits, and has the applicant had a third-party cybersecurity audit in the last twelve months? Relatedly, how often does the applicant update its system software, especially anti-virus and anti-malware software, with updates and patches? Also, what insider-threat identification protocols, such as maintaining and reviewing security logs for irregularities or intrusions, does the applicant have in place? What types of passwords

and user logins are required? Does the system require only strong passwords? Does the applicant allow remote access to its network? Does the applicant allow for wireless network connectivity? If so, what protections are employed? Finally, the insurer should do all it can to know exactly what the applicant does with respect to encryption and firewalls.

7. Physical Vulnerabilities. Another aspect of data infrastructure security of which underwriters need to be aware are the protections put in place by the applicant with respect to its servers and its offices. For instance, underwriters should inquire about whether the servers are monitored by video surveillance and have an understanding of physical access controls to the applicant's building and offices, such as keycards and biometrics.

8. Human Vulnerabilities. A critical component of the applicant's data security is the training it provides to employees regarding the handling of sensitive information. Too many data breaches are simply the product of inadvertent conduct or human error. Moreover, underwriters need to inquire about the policies and procedures in place for an employee's access once he/she leaves the company.

9. Contractors and Vendors. As discussed above, insurers should also be keenly aware of the vendors and contractors with whom the applicant does business or to which the applicant outsources its data infrastructure or security functions. This includes whether third-parties host the applicant's network, data storage, and website. To that end, underwriters should inquire whether the applicant requires its vendors to carry cyberinsurance and name the applicant as an additional insured or to indemnify and hold harmless the applicant from the vendors' negligent conduct. Underwriters should also learn whether the applicant requires these third parties to adhere to stringent cybersecurity standards, at least the same ones the applicant adheres to.

10. History of Cyberattacks. Although one attack does not necessarily portend another, an applicant's history of data breach incidents, distributed denial of service attacks, and other security intrusions may indicate whether the applicant may be a high-value target for hackers.

Taken together, these considerations seek to identify the strengths and weaknesses of the applicant's cybersecurity defenses, as well as the applicant's attitude and experience with cybersecurity matters. To put its best case forward and secure a competitive premium, the applicant should assess its network security strength before applying for insurance and leave additional time to incorporate any recommendations by the auditor. In particular, the applicant should allow third-party cybersecurity risk assessors to perform vulnerability scans and penetration tests, focusing on administrative safeguards (policies and procedures limiting access to confidential information), physical safeguards (securing paper records, shredding records with confidential information, and storing servers and laptops in locked areas), and technical safeguards (encryption and firewalls). This process would allow the insurer and applicant to have an open, candid, and productive conversation about the applicant's cyber-risks.


The Cyberliability Insurance Lesson of the Sony Data Breach

History will prove whether *The Interview* Attack was indeed a watershed moment for the cyberinsurance market. Acknowledging the momentum from 2013 to 2014 in terms of cyberinsurance premiums, we are one step closer to the reality foretold by Ari Schwartz, Director of Cybersecurity on the White House National Security Council, who declared that by 2020, "[W]e're going to be well on our way to everyone having cyber insurance as just a basic set of insurance, just like property insurance."

The lesson *The Interview* Attack teaches most importantly is that cyberliability insurance—and not CGL insurance—is the appropriate product for protecting one's business from attacks. As will likely be borne out in the Appellate Division of the Supreme Court of the State of New York in 2015, insurers never intended that CGL insurance cover data breach loss.

Cyberliability insurance is imperative to protect against financially crushing cyberattacks, especially given the propensity for hackers to "copycat" other successful hacks. Accordingly, in response to the ever-present threat of a cyberattack, the pru-

dent move, especially for small, medium, and large-sized companies is to purchase adequate cyberinsurance. Policyholders considering whether to purchase cyberinsurance should not be intimidated by the process of applying for and purchasing these policies. It is presently a soft market, and policyholders have the ability to fully customize their policy package in order to provide a robust "last line of defense" to a cyberattack. Additionally, policyholders need not feel alone in this process. They can and should enlist experienced and knowledgeable brokers and coverage counsel when purchasing these policies.

In the end, if the Target data breach was "the equivalent of 10 free Super Bowl ads" for the cyberinsurance market, *see* Leslie Scism, "Cyberattacks Give Life to Insurance," *Wall Street Journal*, Mar. 26, 2014 (quoting Randy Maniloff of White & Williams), then *The Interview* Attack was like an Academy Award-winning movie. Moreover, it may very well represent the cinematic climax in our move toward a future where cyberliability insurance is a basic coverage for companies operating in an increasingly digital world. 

Stay
connected...



dri™