CYBER INSURANCE 101:
Coverage Issues Related to Cyber Attacks and Cyber Insurance

By Dina M. Cox,[1] Elissa K. Doroff,[2] Kirsten Jackson,[3] Kathryn E. Kasper,[4] and Michael B. Rush[5]

I. The Rise of Cyber Attacks

On October 3, 2013, Adobe Systems Inc., the computer software giant responsible for staple software products such as Adobe Acrobat and Photoshop, announced that its security team had discovered a "sophisticated attack" on its networks, resulting in the exposure of personal information, including the names, passwords, and encrypted credit and debit card numbers, of over 2.9 million Adobe customers.[6] In the weeks following the announcement, this initial

---

[1] Ms. Cox is an attorney at Lewis Wagner, LLP in Indianapolis, Indiana and can be reached at dcox@lewiswagner.com.

[2] Ms. Doroff is a Vice President at Marsh USA, Inc. in New York, New York and can be reached at Elissa.K.Doroff@marsh.com.

[3] Ms. Jackson is an attorney at Kasowitz, Benson, Torres & Friedman LLP in Los Angeles, California and can be reached at kjackson@kasowitz.com.

[4] Ms. Kasper is an attorney at Hancock, Daniel, Johnson & Nagle, P.C. in Richmond, VA and can be reached at kkasper@hdjn.com.

[5] Mr. Rush is an attorney at Potter Anderson & Corroon, LLP in Wilmington, Delaware and can be reached at mrush@potteranderson.com.

[6] Brad Arkin, *Important Customer Security Announcement*, EXECUTIVE PERSPECTIVES, (Oct. 3, 2013), 1:15 PM), http://blogs.adobe.com/conversations/2013/10/important-customer-security-announcement.html.

estimate quickly ballooned to over 150 million, making the breach the largest (in terms of the number of records stolen) publicly disclosed cyber attack to that date.[7] Although Adobe reported that the vast majority of the compromised records were inactive or fictitious accounts, the company set out to notify at least 38 million active users and tens of thousands of inactive users[8], as well as related banks and credit card companies, that their data had been compromised.[9]

As days turned into weeks, the situation proved not only costly, but a public relations nightmare as well. In late November, nearly eight weeks after the breach was disclosed, the company announced that notification was taking longer than expected and some users still had not been advised that their personal information might be at risk.[10] At that point, the stolen information had been circulating the internet – publicly available for anyone to see – for at least three weeks.[11] Because many people use the same passwords across multiple sites, other companies, including Facebook Inc., began reviewing the leaked data for overlapping user information and passwords in order to notify and protect their own customers.[12]

---

[7] Jim Finkle, *Trove of Adobe user data found on Web after breach: security firm*, REUTERS, Nov. 7, 2013, *available at* http://www.reuters.com/article/2013/11/07/us-adobe-cyberattack-idUSBRE9A61D220131107.

[8] Jim Finkle, *Adobe says breach notification taking longer than anticipated*, REUTERS, Nov. 26, 2013, *available at* http://in.reuters.com/article/2013/11/25/adobe-cyberattack-idINDEE9AO0GK20131125.

[9] Arkin, *supra* note 1.

[10] Finkle, *supra* note 3.

[11] *Id.*

[12] *Id.*

To make matters worse, the breach potentially opened the door to a continued threat. Adobe reported that the thieves also stole source code for numerous Adobe products, which computer experts say could allow hackers to find and exploit any other potential weaknesses in the security of those products.[13] This put the users of those programs at risk, as some of the products from which source code was stolen are widely used among businesses and other institutions. As one example, ColdFusion, a web application development software, is used by the United States Senate, 75 of the Fortune 100 companies, and more than 10,000 other companies worldwide.[14] A cyber security breach at any one of these institutions could prove disastrous.

Not surprisingly, little more than a month went by before the first lawsuit was filed against Adobe as a result of this security breach. On November 11, 2013, a proposed class action suit styled *Halpain v. Adobe Systems, Inc.*, was filed in the United States District Court for the Northern District of California, stating causes of action for breach of contract, breach of the covenant of good faith and fair dealing, for money had and received, and for multiple violations of state law.[15] The *Halpain* Complaint alleges that Adobe failed to institute proper security measures to guard personally identifying information (PII) and misrepresented the efficacy of its security protocols.[16] It further contends that Adobe failed to reasonably notify its customers of the breach – alleging that Adobe discovered the breach over two weeks before even announcing

---

[13] David Kocieniewski, *Adobe Announces Security Breach*, N.Y. TIMES, Oct. 3. 2013, *available at* http://www.nytimes.com/2013/10/04/technology/adobe-announces-security-breach.html?_r=0

[14] *Id.*

[15] Complaint at ¶¶ 70-113, *Halpain v. Adobe Systems, Inc.*, No. 5:13-cv-05226 (N.D. Ca. filed November 11, 2013).

[16] *Id*. at ¶ 26.

it.[17] Although the damages sought are undisclosed at this point, given the magnitude of the breach, the potential liability is staggering.

Unfortunately, Adobe is only one among many companies and other organizations which have faced a data breach in the last year alone. The Privacy Rights Clearinghouse, a California nonprofit that maintains a database of reported data breaches, reports that 581 data breaches occurred in 2013, resulting in the disclosure of over 54 million personal records.[18] And although we often think of hackers, like those responsible for the Adobe breach, as the sole factor behind these breaches, the causes are varied and may even come from within the organization itself. The Ponemon Institute, an independent research organization specializing in information security research,[19] reports that in 2012, 35% of data breaches, internationally, were caused by negligent employees or contractors.[20] Within this category, the causes of these breaches range from the loss or improper disposal of electronic devices to inadvertent sharing of information, whether by email or public posting on a website.[21] Only slightly more common were criminal or malicious attacks, accounting for 37% of all international data breaches in 2012.[22] Among these, attacks caused by criminal insiders – employees, contractors, or other third parties – were some of the

---

[17] *Id*. at ¶ 33.

[18] *Chronology of Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/data-breach/new (last visited Jan. 6, 2014).

[19] PONEMON INSTITUTE, http://www.ponemon.org (last visited Jan. 6, 2014).

[20] Ponemon Institute, *2013 Cost of Data Breach Study: Global Analysis*, p. 3 (May 2013), http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf

[21] PRIVACY RIGHTS CLEARINGHOUSE, *supra* note 13.

[22] Ponemon Institute, *supra* note 15, p. 7.

most common.[23] Glitches within computer systems and other business process failures made up the remainder of international data breaches in 2012 – accounting for approximately 29% of such incidents.[24]

The one thing all breaches have in common, however, is the time and expense required to combat their effects. In 2012, the average total organizational cost of a data breach in the United States was over $5.4 million, with an average cost per compromised record of $188.00.[25] An organization presented with a data breach faces the costs of detection of the breach (average cost $395,262), notification to those affected (average cost $565,020), post-breach costs such as legal expenditures and the provision of identity protection services (average cost $1.4 million), and lost business costs (average cost $3 million).[26] Heavily regulated industries, such as the healthcare, finance, and pharmaceutical industries experience the highest costs, with an average cost per record of over $200, but it appears that no sector can afford to overlook the risk of a security breach.[27] In the last year, a wide array of businesses and organizations, ranging from government offices and educational institutions[28] to dating websites[29] and giant retailers,[30] has experienced a data breach in some form or another.

---

[23] *Id.*

[24] *Id.*

[25] *Id.* at 5-6.

[26] *Id.* at 16-17.

[27] *Id.* at 6.

[28] PRIVACY RIGHTS CLEARINGHOUSE, *supra* note 13.

[29] Adam Greenberg, *Millions used '123456' as a password in breach affecting 42 million*, SC MAGAZINE, Nov. 20, 2013, http://www.scmagazine.com/millions-used-123456-as-a-password-in-breach-affecting-42-million/article/321959/

Faced with lawsuits and other costs arising out of these cyber attacks, many companies are turning to their insurance providers for coverage for defense costs and other coverage. However, as many of these businesses and organizations are learning the hard way, coverage under traditional insurance policies for cyber security breaches is no guarantee. The rise in cyber attacks has led to a proliferation of coverage litigation. Two recent examples of such litigation are described below.

A. The Sony PlayStation Cyber-Attack

In *Zurich American Insurance Co., et al. v. Sony Corporation of America, et al.*, N.Y. Supreme Court, New York County, No. 651982/2011 (the "Sony Action"), Zurich is seeking, *inter alia*, a declaration that it has no duty to defend or indemnify numerous Sony Defendants for claims stemming from a massive cyber attack Sony experienced in 2011. As noted below, the parties have filed various dispositive motions, but at the time of the submission of this article, no decisions have been issued.

As part of their business, the Sony Defendants manufacture and sell video game devices, including the PlayStation. In connection with the PlayStation consoles, the Sony Defendants operate and maintain several online gaming/entertainment networks, including the PlayStation Network ("PSN"). The PSN allows consumers to play video games on-line against other users, and also allows consumers to purchase and download games, music, movies and other content to their PlayStation. Although credit card information is not needed for some services, consumers need to enter that information to purchase content.

---

[30] Anne D'Innocenzio & Bree Fowler, *Target security breach affects up to 40M cards*, MSN MONEY, Dec. 19, 2013, http://money.msn.com/business-news/article.aspx?feed=AP&date=20131219&id=17206131&ocid=ansmony11

Between April and June 2011, computer hackers unlawfully gained access to the PSN and other networks operated by the Sony Defendants. The various intrusions resulted in the unauthorized access to and theft of personal and financial information of over 100 million PSN customers. In the aftermath of the attacks, the Sony Defendants found themselves named as defendants in 55 class action complaints filed in the United States and three class action lawsuits filed in Canada. In general, the underlying complaints allege that Sony failed to take adequate steps to protect the underlying plaintiffs' information, and that Sony unreasonably delayed notifying consumers of the cyber attack and resulting theft of information. The underlying plaintiffs further allege that they suffered damages as a result of the shutdown of the PSN following the cyber attacks. The Sony Defendants provided notice of the claims asserted in the various actions to Zurich, but Zurich denied it had a duty to defend and thereafter instituted the insurance action.

The Sony Defendants have filed a motion for partial summary judgment, seeking a ruling that Zurich owes them a duty to defend. The Sony Defendants argue that the policies provide coverage for damages because of "personal and advertising injury," which includes "oral or written publication, in any manner, of material that violates a person's right of privacy." The Sony Defendants claim that the underlying complaints trigger this coverage by virtue of seeking damages arising out of the unauthorized disclosure of private, personal, and/or confidential information.

Among the issues to be argued include whether the "publication" aspect of the policy's provisions can be met even where the customer information is not formally published in any location (*i.e.*, it was not released on a website, etc.). Additionally, the Sony Defendants argue that an Internet Business Exclusion in the policy does not apply to preclude coverage. That

exclusion excludes coverage for an insured whose business is, *inter alia*, "An Internet search, access, content or service provider." Whether the Sony Defendant's hosting of content on the PSN renders it an Internet Business will be an issue decided in the litigation.

B. The Michaels Stores Attack

The insurance issues discussed herein do not necessarily have to arise out of traditional "hacking." Instead, many of the same issues can arise out of similar situations in which customer's personal data is stolen by a third party. For instance, in *Arch Insurance v. Michaels Stores, Inc.*, No. 12-0786, N.D. Ill., Arch sought a declaration that it had no duty to defend Michaels in underlying actions stemming from the theft of consumers' credit and debit card information. The theft of data in this case arose when pin pads at store registers were tampered with to allow for the theft of data to occur.[31] The policy at issue excluded electronic data from the definition of tangible property. As a result, the focus was on the publication of materials clause. Although the issue was briefed, the parties reached a settlement agreement prior to a decision being issued.

II. Coverage Issues Under CGL Policies

A. Covered Property

Under the typical CGL policy, loss of electronic data may not be covered property. This is because the standard 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

[31] The attack Michaels experienced in late 2010 is similar to the one Target experienced during the 2013 holiday season. *See* *http://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/index.html?iid=EL* (last visited on January 7, 2014).

damage'."[32] The standard definition of "property damage," in turn, 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."[33] Thus, insurers typically argue that data is not "tangible property" that can suffer "physical injury" as defined by the policy.

This argument, however, is not always successful. In *Retail Systems, Inc. v. CNA Insurance Companies,* for example, the Court of Appeals of Minnesota held that coverage existed under a traditional CGL policy where the insured lost a computer tape containing the data belonging to a third party.[34] When the third party consequently sued the insured for the loss, the insured attempted to tender defense of the action to CNA.[35] CNA refused to defend, citing the definition of property damage contained in the policy – "physical injury or destruction of tangible property" – and arguing that the lost tape and data were not "tangible property."[36] The Court held that the term "tangible property" was ambiguous, and as such, must be construed in favor of the insured.[37] Additionally, the Court found that multiple considerations supported the conclusion that the tape and the data contained thereon were "tangible property" under the policy.[38] The data on the tape, the Court stated, "was of permanent value and was integrated completely with the physical property of the tape," such that the physical loss of the tape was

---

[32] ISO Form CG 00 01 04 13 (2012), Section I, Coverage A, § 1.a.

[33] ISO Form CG 00 01 04 13 (2012), Section V, § 17.

[34] 469 N.W.2d 735 (Minn. Ct. App. 1991).

[35] *Id.* at 736-37.

[36] *Id.* at 737.

[37] *Id.*

[38] *Id.*

also a physical loss of the data.[39] The Court also expressly rejected tax cases holding that computer tapes were "intangible property" as inapposite to the case at hand, explaining that:

> Because data can be removed from a computer tape at any time, the transfer of the physical property (the tape) is only incidental to the purchase of the knowledge and information stored on the tape. Thus, the tape has little value for tax purposes. But if the tape is lost while it still contains the data, as is the case here, its value is considerably greater.[40]

On the other end of the spectrum, in *America Online, Inc. v. St. Paul Mercury Insurance Co.*,[41] the Fourth Circuit upheld a denial of coverage where third parties claimed that AOL's software caused loss of data and damage to their personal computers. St. Paul denied coverage for the actions under AOL's professional liability policy, claiming that the alleged damages did not fall within the policy's definition of "property damage," defined as "physical damage to tangible property."[42] Applying Virginia law, the Court agreed with St. Paul and held that data is "abstract and intangible", such that damage to data cannot be damage to "tangible property."[43] The Court distinguished the data contained on a hard drive from the hard drive itself, explaining that if the hard drive were physically damaged (*e.g.*, scratched) so that it could no longer record information, this damage would be covered.[44] However, damage merely to the information that

---

[39] *Id.*

[40] 469 N.W.2d at 738.

[41] 347 F.3d 89 (4th Cir. 2003).

[42] *Id.* at 92.

[43] *Id.* at 96.

[44] *Id.* at 95.

did not affect the physical processes of the hard-drive was not physical damage to tangible property, and thus, was not covered damage under the policy.[45]

Likewise, in *Ward General Insurance Services, Inc. v. Employers Fire Insurance Co.*,[46] the California Court of Appeals held that there was no coverage where a computer system crash resulted in the loss of the insured's electronically stored data. Faced with restoration costs, such as hiring consultants and manually re-entering the lost data, the insured made a claim with Ward under its Building and Personal Property coverage.[47] Ward denied the claims, contending that the policy required "direct physical loss of or damage to Covered Property" and the loss of data was not a "physical loss."[48] The Court in that case looked to the ordinary meaning of the word "physical," which it found mean, *inter alia*, "having material existence."[49] "Data," on the other hand, was defined as "factual or numerical information."[50] From these definitions, the Court concluded that "information" did not have a "material existence" such that it could suffer "physical" damage within the meaning of the policy.[51]

In light of this contrasting case law, many insurance companies have adapted their CGL forms to expressly eliminate any possibility of coverage for data loss. The ISO has amended the definition of "property damage" contained in its CGL form to clarify that "electronic data is not

---

[45] *Id.*

[46] 7 Cal. Rptr. 3d 844 (Cal. Ct. App. 2003).

[47] *Id.* at 550.

[48] *Id.* at 551.

[49] *Id.* at 557.

[50] *Id.*

[51] *Id.* at 850-51.

tangible property."[52] The form was amended again in 2004 to exclude from property damage coverage any "[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."[53]

Although these changes have greatly limited coverage for data loss under traditional CGL policies, coverage for related claims has not been completely foreclosed. In *Eyeblaster, Inc. v. Federal Insurance Co.,*[54] for example, the Eighth Circuit left open the possibility of coverage for claims related to poor computer performance.[55] The underlying complaint in that case alleged that Eyeblaster infected the complainant's computer with spyware, which slowed computer processes and sometimes resulted in crashes.[56] Eyeblaster tendered defense of the action to Federal under its CGL policy, but Federal denied coverage, arguing that the complaint did not allege "property damage," which was defined in the policy 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" and expressly excluded "any software, data or other information that is in electronic form."[57] The Court concluded that "[t]he plain meaning of tangible property includes computers, and the [underlying] complaint alleges repeatedly the 'loss of use' of his

---

[52] Jean-Paul Jaillet, *Insurance Coverage for Cyber-Risky Business*, LAW 360, Feb. 21, 2012, *available at* http://www.choate.com/uploads/103/doc/jaillet-insurance-coverage-for-cyber-risky-business.pdf

[53] *Id.*

[54] 613 F.3d 797 (8th Cir. 2010).

[55] *Id.* at 802-03.

[56] *Id.* at 800.

[57] *Id.* at 801-02.

computer," such that Federal had a duty to defend Eyeblaster under the policy.[58] Thus, whether damage is covered may depend on how the damage is framed – while "data loss" will be excluded, damages related to computer hardware, which may in effect be the same, may be covered under the traditional CGL policy.

B. Publication Issues: In General

The Personal and Advertising Injury provisions of a standard CGL policy may provide coverage in data-related incidents, but whether this is the case will often depend on the jurisdiction and specific policy language at issue. The typical language contained in such provisions states that the insurer will pay for damages caused by "[o]ral or written publication, in any manner, of material that violates a person's right of privacy."[59] Consequently, the key issue in a coverage determination suit is generally whether there has been a "publication" that violates the claimant's "right of privacy" – both terms which are left undefined by the policy. Opinions diverge on this issue, with some courts holding that "publication" requires that information be transmitted to a third party, while other courts construe the term more broadly to encompass nearly any transmission of information.

Falling into the former category, the Ninth Circuit upheld coverage under a CGL policy in *Netscape Communications Corp. v. Federal Insurance Co.*.[60] In that case, Netscape sought defense and indemnity from Federal in connection with a suit brought by Netscape users alleging that Netscape's SmartDownload software violated the users' privacy by collecting, storing, and

---

[58] *Id.* at 802.

[59] ISO Form CG 00 01 10 01 (2000), Section V, § 14.

[60] 343 Fed.Appx. 271 (9th Cir. 2009)

disclosing to Netscape information about the users' internet usage.[61] The policy at issue provided coverage for "personal injury offense[s]," which included "[m]aking known to any person or organization written or spoken material that violates a person's right to privacy."[62] In an opinion spanning little more than a page, the Ninth Circuit – noting that coverage provisions are to be broadly construed under California law – held that the underlying complaint sufficiently alleged that Netscape had committed a "personal injury offense" within the definition of the policy by intercepting and internally disseminating private online communications.[63] The fact that the language of the relevant provision stated that disclosure to "any" person or organization, the court stated, was the dispositive factor.[64]

In a similar vein, the United States District Court for the District of Maryland held in *Zurich American Insurance Co. v. Fieldstone Mortgage Co.*[65] that Zurich had a duty to defend its insured, Fieldstone, where Fieldstone was accused of improperly accessing and using consumer credit information in violation of the Fair Credit Reporting Act. The underlying complaint in that case alleged that Fieldstone accessed the complainants' consumer credit reports without a permissible purpose under the FCRA in order to use information to extend "prescreened" credit offers to the complainants.[66] Fieldstone tendered defense of the suit to Zurich under its

---

[61] *Netscape Communs. Corp. v. Fed. Ins. Co.*, 2007 U.S. Dist. LEXIS 78400, *3-4 (N.D. Ca. Oct. 10, 2007).

[62] *Id.* at *5.

[63] 343 Fed.Appx. at 272.

[64] *Id.*

[65] 2007 U.S. Dist. LEXIS 81570, *2 (D. Md. Oct. 26, 2007).

[66] *Id.*

commercial general liability policy which provided that Zurich would "pay those sums that [Fieldstone] becomes legally obligated to pay as damages because of personal and advertising injury."[67] "Personal and advertising injury" was defined in the policy to include "[o]ral or written publication, in any manner, of material that violates a person's right of privacy."[68] The court, applying Maryland law, noted that the word "publication" was not defined in the policy and, thus, interpreted the policy using the ordinary meaning of the word – which it found to be "the act of publishing, or to produce or release for distribution."[69] Using this definition, the court held that the printing and mailing of written solicitations – that is, the sending of the prescreened offers – constituted "publication" within the meaning of the policy.[70] The court expressly rejected Zurich's argument that "publication" requires that the allegedly private information be divulged to a third party, distinguishing the language at issue in that case – publication in any manner – from cases where the relevant policy required that the information be "made known."[71] "Making known," the court stated, implies discovery or a previous ignorance, which would necessitate disclosure to an unaware third party; "publication," however, carries no such connotation.[72] Notably, the policy at issue in *Netscape* used the "make known" language and yet the Ninth Circuit still found coverage under similar facts.[73]

---

[67] *Id.* at *3.

[68] *Id.* at *3-4.

[69] *Id.* at *12 (*citing* Merriam-Webster's Collegiate Dictionary 1006 (11th ed. 2003)).

[70] *Id.* at *13.

[71] 2007 U.S. Dist. LEXIS 81570 at 15.

[72] *Id.*

[73] 2007 U.S. Dist. LEXIS 78400 at *5; 343 Fed.Appx. at 272.

Likewise, in *Pietras v. Sentry Insurance Co.*,[74] the United States District Court for the Northern District of Illinois upheld coverage under facts nearly identical to those in *Fieldstone*. As in *Fieldstone*, the underlying claim in *Pietras* involved allegations that Sentry's insured had improperly accessed consumer credit reports in violation of the FCRA and subsequently mailed solicitations for "pre-approved auto loans" to individuals whose credit reports had been accessed.[75] Also like *Fieldstone*, the CGL policy at issue provided coverage for "personal and advertising injury" which included "oral or written publication of material that violates a person's right to privacy."[76] Relying on the Illinois Supreme Court opinion in *Valley Forge Insurance Co. v. Swiderski Electronics, Inc.*,[77] in which that court held that a single fax transmission to a single recipient constituted "publication," the District Court concluded that

> "publication" in a policy providing coverage for "advertising injury" includes communication to as few as one person, thereby resulting in coverage for violations of a statute invoking privacy interests, such as the FCRA.[78]

Thus, the FCRA allegations in the underlying complaint fell within the "advertising injury" provision of the policy and Sentry was, accordingly, obligated to defend its insured against these claims.[79]

Because of its reliance on *Valley Forge*, however, the reasoning underlying the District Court's opinion in *Pietras* was somewhat different than that underlying the opinion of the

---

[74] 2007 U.S. Dist. LEXIS 16015 (N. D. Ill. Mar. 6, 2007).

[75] *Id.* at *2.

[76] *Id.*

[77] 860 N.E.2d 307 (Ill. 2006).

[78] 2007 U.S. Dist. LEXIS 16015 at *10.

[79] *Id.* at 11.

District Court for the District of Maryland in *Fieldstone*, despite the fact that the two cases were nearly factually identical. This is because *Valley Forge*, and other cases concerning alleged violations of the Telephone Consumer Protection Act (TCPA),[80] deal not only with the "publication" issue, but also whether the alleged publication has implicated a "right of privacy" under the policy. In *Valley Forge*, for example, the underlying complainant alleged that Valley Forge's insured, Swiderski, sent the complainant unsolicited facsimile advertisements in violation of the TCPA.[81] Similar to the provision contained in *Pietras*, the Valley Forge policy provided coverage for "personal and advertising injury" including "[o]ral or written publication, in any manner, of material that violates a person's right of privacy."[82] Based on this language, Valley Forge argued that the "right of privacy" was only implicated where the *content* of the published material somehow violated a claimant's right to privacy.[83] The court, however, rejected this argument, holding that "the receipt of an unsolicited fax advertisement implicates a person's right of privacy insofar as it violates a person's seclusion, and such a violation is one of the injuries that a TCPA fax-ad claim is intended to vindicate."[84] The court then looked to the plain meaning of the word "publication" – defined as communication or distribution of copies to the public[85] – to conclude that the fax advertisements had been published in violation of the claimant's right of privacy and, thus, the claim fell within the coverage of the "advertising

---

[80] 47 U.S.C. § 227.

[81] 860 N.E.2d at 310.

[82] *Id.* at 310-11.

[83] *Id.* at 313.

[84] *Id.* at 315.

[85] *Id.* at 316 (*citing* Webster's Third New International Dictionary 1836 (2002)).

injury" provision.[86] The United States Court of Appeals for the Tenth Circuit,[87] the Supreme Court of Florida,[88] and the Supreme Court of Missouri[89] have all held similarly.

On the other end of the spectrum, some courts have denied coverage under the "personal and advertising injury" provisions of the typical CGL policy, holding that "publication" under such a policy requires disclosure to a third party. The Eleventh Circuit, for example, in *Creative Hospitality Ventures, Inc. v. United States Liability Insurance Co.*,[90] was faced with a situation in which an insured was alleged to have issued sales receipts to customers revealing more than five digits of the customer's credit card number or the card's expiration date in violation of the Fair and Accurate Credit Card Transaction Act (FACTA).[91] The policy in that case, like many of those cited above, defined "personal and advertising injury" to include "[o]ral or written publication, in any manner, of material that violates a person's right of privacy."[92] Relying on the definition of "publication" set forth by Supreme Court of Florida in *Penzer v. Transportation Insurance Co.*[93] (a TCPA case) – communication to the public or the act or process of issuing copies for general distribution to the public – the Court of Appeals held that there was no

---

[86] 860 N.E.2d at 317.

[87] *Park Univ. Enters. v. Am. Cas. Co.*, 442 F.3d 1239 (10th Cir. 2006).

[88] *Penzer v. Transp. Ins. Co.*, 29 So. 3d 1000 (Fla. 2010).

[89] *Columbia Cas. Co. v. Hiar Holding, L.L.C.*, 411 S.W.3d 258 (Mo. 2013).

[90] 444 Fed. Appx. 370 (11th Cir. 2011).

[91] 15 U.S.C. § 1681c(g)(1).

[92] 444 Fed. Appx. at 371.

[93] 29 So. 3d 1000 (Fla. 2010).

"publication" in this case.[94] "[P]roviding a customer a contemporaneous record of a retail transaction," the court stated, "involves no dissemination of information to the general public" as the receipt is provided only to the customer him or herself.[95] The court also expressly rejected the insured's argument that the inclusion of the phrase "in any manner" in the definition of "publication" within the policy – which was not present in the policy at issue in *Penzer* – somehow expanded that definition.[96] The court explained that the phrase merely expanded the categories of publication (such as email, handwritten letters, or "blast-faxes"), and did not change the plain meaning of the underlying term "publication."[97]

Similarly, in *Whole Enchilada Inc. v. Travelers Property Casualty Company of America,*[98] the United States District Court for the Western District of Pennsylvania denied coverage where the underlying complaint alleged violations of FACTA. The policy at issue in that case, pursuant to a WEB XTEND endorsement, provided that "personal and advertising injury" included "[o]ral, written or electronic publication of material that appropriates a person's likeness, unreasonably places a person in a false light or gives unreasonable publicity to a person's private life."[99] Whole Enchilada argued that the underlying complaint alleged "publication" of material that both "appropriates a person's likeness" and "gives unreasonable

---

[94] 444 Fed. Appx. at 375-36.

[95] *Id.* at 376.

[96] *Id.*

[97] *Id.*

[98] 581 F. Supp. 2d 677 (W.D. Pa. 2008).

[99] *Id.* at 693.

publicity to a person's private life."[100] The court, addressing each of these arguments in turn, found none availing.[101] Relying on the dictionary definition of "publication" the court held that the underlying complaint did not allege that Whole Enchilada was liable for publication, as the receipts were given only to the customer herself and not "made generally known, publicly announced, nor disseminated to the public."[102] The court similarly relied on the dictionary definition of "likeness" to reject Whole Enchilada's contention that the receipts "appropriate[d] a person's likeness."[103] "[E]ven if financial identity equated with a person's 'likeness' as Whole Enchilada suggests," the court stated, the underlying complaint alleged only that Whole Enchilada failed to protect customers from credit or debit card fraud, and did not allege any use of that information.[104] The court also rejected Whole Enchilada's argument that the complaint gave "unreasonable publicity to a person's private life," relying on both the dictionary definition of the word, as well as Pennsylvania case law construing the meaning of the word "publicity" to conclude that the underlying complaint did not allege that Whole Enchilada displayed the claimants' information to the public or took any action designed to disseminate the information to the public at large.[105] In doing so, the court also expressly distinguished *Fieldstone* and *Park*

---

[100] *Id.* at 696.

[101] *Id.* at 697, 698, 699.

[102] *Id.*

[103] *Id.* at 698.

[104] 581 F. Supp. 2d at 698.

[105] *Id.* at 699.

stating that, unlike alleged violations of the FCRA and the TCPA, an alleged violation of FACTA did not protect or otherwise implicate a privacy right.[106]

C. Other Publication Issues

Among the many issues that might arise in litigation over whether coverage exists are disputes involving the word "publication." As noted above, the most likely source of coverage in the aftermath of a cyber attack in a CGL policy are provisions that provide for coverage of injuries arising from the publication of material that violates a person's right of privacy. This might include situations where customer's credit or debit card information was stolen.

Other disputes over the term "publication" arise in two notable situations: (1) disputes over whether the policy requires the "publication" be made by the insured, as opposed to a third party; and, (2) disputes about how widespread the "publication" must be in order to implicate coverage.

1. Publication by Whom?

As illustrated by some of the case studies discussed above, in the typical cyber attack, the insured is an innocent victim. Although questions may exist as to whether the insured utilized adequate safeguards to protect customer data or other confidential information, in general, the insured is not responsible for the theft of the data or any illicit use of the stolen data. However, the fact that any publication is caused by a third party (*i.e.*, the hacker) has led insurers to take the position that coverage is unavailable.

Under the insurers' position, "Coverage B Personal and Advertising Injury Liability" only extends to injuries arising from the insured's conduct and focuses on whether the insured's conduct amounts to a covered offense. For instance, in *Butts v. Royal Vendors, Inc.*, after

---

[106] *Id.* at 700-01.

concluding that coverage existed on separate claims, the West Virginia Supreme Court of Appeals held that the insured's alleged liability for inducing the underlying plaintiff's (a former employee) physician to breach his fiduciary duty was outside coverage for oral or written publication of material that violated a person's right to coverage.[107] Without providing any analysis, the court concluded that to invoke coverage under this policy section, the underlying plaintiff "would need to set forth an allegation that Royal Vendors published material that invaded his privacy."[108] Instead, the underlying complaint alleged that Royal Vendors *induced* the underlying plaintiff's doctor to publish material that violated the underlying plaintiff's right to privacy.[109] The court held that the "policy was not written to cover publication by a third-party" and no coverage existed with respect to this claim.[110] Other courts have reached similar rulings with respect to other types of personal and advertising injuries.[111]

Conversely, in addition to attempting to distinguish cases cited by the insurers, insureds typically rely on the language of the policy in arguing that coverage is not limited to publications by the insured. First, as noted above, the provision in question reads: "[o]ral or written publication, ***in any manner***, of material that violates a person's right of privacy."[112] Insureds

---

[107] *Butts v. Royal Vendors, Inc.*, 504 S.E. 2d 911, 917 (W.Va. 1998).

[108] *Id.*

[109] *Id.*

[110] *Id.*

[111] *See Dryden Oil Co. of New England, Inc. v. Travelers Indem. Co.*, 91 F.3d 278, 286 (1st Cir. 1996) ("personal injury liability coverage obligates the insurer to indemnify for liability incurred for certain intentional acts by the insured"); *County of Columbia v. Continental Ins. Co.*, 83 N.Y. 2d 618, 627 ("coverage under the personal injury endorsement provision in question was intended to reach only purposeful acts undertaken by the insured or its agents.").

[112] *See, e.g.*, ISO Form CG 00 01 12 07 at pg. 14 (emphasis added).

will argue that the inclusion of the bolded phrase indicates that coverage should be interpreted broadly.[113] This is consistent with a general principal that coverage clauses should be interpreted broadly.[114] Insureds also point to the fact that various exclusions to the "Personal and Advertising Injury" coverage explicitly exclude coverage for injuries caused by conduct carried out "by or at the direction of the insured." For example, one exclusion states that coverage does not apply to:

> **a. Knowing Violation of Rights of Another**- "Personal and advertising injury" caused by or at the direction of the insured with the knowledge that the act would violate the rights of another and would inflict "personal and advertising injury."[115]

In light of this limiting language, insureds will argue that the insurers' interpretation that coverage never extends to injuries caused by third parties would render the limiting language superfluous.[116]

2. *Extent of Publication?*

Another issue likely to arise in the aftermath of a hacking incident is to what extent, if at all, publication of customer or other confidential data occurred. On one end of the spectrum, the hackers could take the stolen data and post it on a blog, message

---

[113] *See Nat'l Gypsum Co. v. Prostok*, 2000 WL 1499345, at *20 (N.D. Tex. Oct. 5, 2000) ("The word 'any' is a broad word. 'A more comprehensive word than 'any' could hardly be employed. It means indiscriminate, or without limitation or restriction.'") (*quoting Commonwealth v. One 1939 Cadillac Sedan*, 45 A 2d 406, 409 (Pa.Super.1946)).

[114] *See Sun-Times Media Group, Inc. v. Royal & Sunalliance Ins. Co. of Canada*, 2007 WL 1811265, at *11 n.65 (Del. Super. June 20, 2007) ("grants of coverage must be interpreted broadly in favor of the existence of insurance while limitations thereon, or exclusions, must be interpreted narrowly against the insurance company").

[115] *See, e.g.,* ISO Form CG 00 01 12 07 at pg. 6 (emphasis in original).

[116] CITE

board, or other website. On the other end of the spectrum, the hackers might not publish the data for widespread consumption, but instead might use the stolen data for their own personal gain. One additional possibility exists under which the data is stolen, but never used for one reason or another.

Insurers are likely to take a strict interpretation of the term "publication" and argue that in order for a duty to defend to be triggered, the underlying lawsuits must allege that actual publication of the stolen information occurred (as opposed to merely illicit use of the information). Similarly, insurers will likely argue that the alleged "publication" must be widespread and will cite to cases stating that "publication" is defined as a communication to the public.[117]

Conversely, and not surprisingly, insureds are likely to argue that the size of the "publication" is irrelevant. Instead, "publication" can occur when disclosure of the information is made to a small group of people or even a single person.[118]

There do not appear to be any cases in which a court discusses the extent to which publication must occur in the hacking context.

D. Intentional Acts or Accidents?

---

[117] *See, e.g., Penzer v. Transp. Ins. Co.*, 29 So.3d 1000, 1005-06; *Nutmeg Ins. Co. v. Employers Ins. Co. of Wausau*, 2006 WL 453235, at *9 (N.D. Tex. Feb. 24, 2006) ("'Publish' generally means 'to disclose, circulate, or prepare and issue printed material for public distribution.'")

[118] *See, e.g., LensCrafters, Inc. v. Liberty Mut. Fire Ins. Co.*, 2005 WL 146896 (N.D. Cal. Jan. 20, 2005) (publication occurred where information was shared with a small group of people); *Tamm v. Hartford Fire Ins. Co.*, 2003 WL 21960374, at **3-4 (Mass. Super. July 10, 2003) (finding that "publication" occurred where information was shared with a small group of people);

Another issue that arises less frequently in cyber cases is whether coverage is excluded because the underlying injury was caused by an intentional act. This issue can arise over questions as to whether a third party's attack triggers the exclusion or in situations where the dispute centers around an intentional act with allegedly unintended results.

In *Lambrecht & Associates v. State Farm Lloyds*, the Texas Court of Appeals reversed the lower court's granting of summary judgment to the insurer.[119] In this case, Lambrecht, an employment agency, encountered issues when its server contracted a computer virus that prevented employees from inputting or retrieving data from the computer system.[120] The virus forced Lambrecht to replace the server. Lambrecht submitted claims for: (1) the value of lost property, comprised of (a) the value of the server, and (b) the value of the software installed on the server; and (2) income lost due to business interruption, comprised of (a) Lambrecht's inability to conduct business when the server was inaccessible, and (b) time lost due to replacing information on the server.[121] State Farm denied coverage.[122]

Among the issues addressed by the court was whether the conduct causing the loss was intentional, which would bar coverage under the policy.[123] State Farm argued that coverage was excluded because the actions of the hacker were intentional.[124] The court disagreed and found that Lambrecht's contracting the computer virus was accidental rather than intentional.

---

[119] *Lambrecht & Associates v. State Farm Lloyds*, 119 S.W.3d 16 (Tex. Ct. App. 2003)

[120] *Id*. at 19.

[121] *Id*.

[122] *Id*.

[123] *Id*. at 21.

[124] *Id*.

Specifically, the court concluded that intentionality is determined from the viewpoint of the insured, and State Farm failed to present evidence that Lambrecht intentionally downloaded the computer virus or committed any acts that Lambrecht would reasonably believe resulted in contracting the computer virus.[125] Thus, the lower court's entry of summary judgment was improper and was reversed.[126]

Santos v. Peerless Insurance Company presented a different situation.[127] Here, Santos was the party causing the cyber injury, and although there was no dispute that he acted intentionally, he claimed Peerless was obligated to provide coverage to him because he did not intend the results that occurred.[128] The insurance dispute arose after Apple Computer filed claims against Santos alleging that he attempted to infiltrate Apple's information systems by sending repeated information requests to Apple through its website, which caused a slowdown and loss of capacity of Apple's servers. Santos tendered the claims to Peerless, who denied coverage.

There was no dispute that Santos acted intentionally by sending requests to Apple's servers. However, Santos claimed that he did not intend to cause Apple's servers to slow down or lose any capacity. Although the court agreed that intentional conduct could cause accidental results for insurance purposes in some cases (*i.e.* hitting a baseball that accidentally breaks a window), in this case Santos intentionally bombarded Apple's servers in order to procure information (to which he was not entitled), and thus the unforeseen damage to Apple's server

---

[125] *Id*. at 21-22.

[126] *Id*. at 27.

[127] *Santos v. Peerless Insurance Company,* 2009 WL 1164972 (Cal. Ct. App. Apr. 30, 2009).

[128] *Id*. at *3.

could be tied to the intentional conduct. Accordingly, the policy excluded damages due to slowdown and loss of capacity of Apple's server.

III. Errors and Omissions Coverage

A. Overview

Errors and omissions policies cover claims arising from negligent acts or failure to provide the level of advice or service that was expected. Most errors and omissions policies are claims-made,[129] meaning they limit coverage to claims made during the policy period. Some errors and omissions policies limit coverage to claims reported during the policy period.

Many errors and omissions policies specify a retroactive date in the declarations. Generally, the retroactive date should be the inception date of the first claims-made errors and omissions policy. If a retroactive date is provided, then the policy will cover a claim only if it results from an act, error, or omission that was committed on or after that date. The retroactive date should remain the same each time the policy is renewed.

Cyber insurance policies, with respect to third-party claims, generally cover crisis management expenses, such as the costs of notifying affected parties, costs of providing credit monitoring to affected parties, costs of public relations consultants, forensic investigation costs incurred to determine the existence or cause of a breach, regulatory compliance costs, costs to pursue indemnity rights, and costs to analyze the insured's legal response obligations.[130] They may also cover claim expenses, such as the cost of defending lawsuits and judgments and

---

[129] Marianne Bonner, *Who Needs Errors and Omissions Liability Coverage?*, ABOUT.COM, http://businessinsure.about.com/od/liabilityinsurance/fl/Who-Needs-Errors-and-Omissions-Liability-Coverage.htm.

[130] SIEMENS AND BECK ON OBTAINING OPTIMAL CYBER INSURANCE, 2012 Emerging Issues 6613 (2012).

settlements.[131] Additionally, cyber insurance policies may cover regulatory response costs, such as the cost of responding to regulatory investigations and costs associated with settling regulatory claims.[132]

Cyber insurance policies may also cover certain first-party claims. This coverage can include the costs of restoring, recreating, or collecting lost data, stolen data, and damaged data.[133] Such policies may also cover revenue lost due to the interruption of operations caused by, for example, hacking, virus transmission, and other security failures.[134] Some policies also cover costs associated with responding to "e-extortion" threats or demands for "ransom" to prevent a threatened cyber attack.

Compared with commercial general liability policies, errors and omissions policies are generally broader in scope. Generally, it is easier to obtain coverage for cyber liability claims under an errors and omissions policy compared with a commercial general liability policy. For example, errors and omissions policy claims are not limited to publications that violate the right of privacy with respect to personal and advertising injury liability coverage. Errors and omissions policies may also bridge coverage gaps in commercial general liability policies.[135] To illustrate, errors and omissions policies are available for software, information technology (IT) services, and e-commerce business, which may bridge "loss of use" gaps in commercial general liability policies that may not cover "impaired products."

---

[131] *Id*.

[132] *Id*.

[133] *Id*.

[134] *Id*.

[135] Bert Wells et al., APPLEMAN ON INSURANCE § 29.04 (2013).

As a reminder, errors and omissions policies are not general liability policies; thus, they are unlikely to cover all claims arising from the insured's business interactions. In contrast, technology errors and omissions policies generally cover two basic risks: (1) financial loss of a third party arising from failure of the insured's product to perform as intended or expected and (2) financial loss of a third party arising from an act, error, or omission committed in the course of the insured's performance of services for another. [136]

B. Specific Issues Affecting Coverage

Errors and omissions policies require an act of negligence. These policies generally provide coverage only for claims arising from "unintentional omissions" or "negligent" acts, meaning they exclude coverage for claims arising from intentional acts by the insured. Acts, errors, and omissions are only covered "wrongful acts" when committed "in the course of the insured's performance of services for another."[137] Definitions matter: An insured will want a policy with a comprehensive definition of services to encompass all products and services expected or likely to be provided during the course of the policy period. Errors and omissions policies for technology companies may include coverage for negligence in failing to maintain confidentiality or security of customer information, invasion of privacy, unauthorized access or use, or introduction of malicious code.

Generally, errors and omissions policies do not cover intentionally wrongful acts, and may also exclude reckless acts. To illustrate, if a company has a duty to notify affected parties and fails to do so, it may be found to have engaged in an intentional act or willful or malicious

---

[136] IRMI Online Glossary, INT'L RISK MGMT. INST., http://www.irmi.com/online/insurance-glossary/terms/t/technology-errors-and-omissions-insurance-tech-eo.aspx.

[137] Bert Wells et al., APPLEMAN ON INSURANCE § 29.04 (2013).

conduct such that coverage is denied. Cyber risks may involve hackers and other criminal actors involved in intentional wrongdoing.[138]

Errors and omissions policies generally contain an "expected" or "intended" exclusion, which prevents coverage for expected or intended acts. The exclusion usually requires the policyholder to intend the specific damage caused. Some courts hold that intentional conduct, even when it causes unintended consequences, cannot be considered a wrongful act that would trigger coverage under an errors and omissions policy. Other courts hold that an insurer must still defend an insured for intentional acts resulting in unintended damages when the policy does not exclude coverage for intentional acts resulting in unintended damages.[139]

A rogue employee's intentionally wrongful acts are not necessarily imputed to the employer for the purposes of applying the exclusion.[140]

Coverage may depend on the policy's definition of covered activities.[141] An errors and omissions policy may provide coverage for malfunction of insured's software, which results in a third party's loss of use of their computers or networks. The policy may provide coverage for data losses attributable to the insured's acts and omissions. Some policies limit coverage to specific conduct or narrowly specified professional services. Thus, ancillary services, such as marketing and administrative actions, might not be covered by the policy. By comparison, some

---

[138] Nancy D. Adams et al., *Cloud Cover: Insuring Technology & Cyberliability Risks*, ABA SEC. OF LIT. 2012 INS. COVERAGE LIT. COMM. (Oct. 18, 2012).

[139] *See, e.g.*, *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797 (8th Cir. 2010) (finding greater likelihood for coverage when company's professional services involved handling data or other tech-related activity).

[140] Bert Wells et al., APPLEMAN ON INSURANCE § 29.04 (2013).

[141] SIEMENS AND BECK ON OBTAINING OPTIMAL CYBER INSURANCE, 2012 Emerging Issues 6613 (2012).

policies are broadly written to cover all of the insured's business activities (or they are ambiguously written such that the policy is construed in favor of coverage).

Additionally, errors and omissions policies may exclude privacy claims. Errors and omissions policies in the cyber context are generally designed to cover loss from errors or omissions or product failures that result in damage to third parties, negligent errors or misstatements, faulty software development, web hosting, internet consulting, computer viruses, and intellectual property infringement.[142] Errors and omissions policies cover losses stemming from the insured's products and services as long as the cause of the loss is covered.

Instead of privacy claims, errors and omissions policies generally focus on four areas:[143] (1) security; (2) advertising and personal injury; (3) electronic activity liability; and, (4) in some instances, infringement on intellectual property. Many costs incurred by the insured company are either first-party losses or involve activity undertaken prior to a "claim" being made, such as providing notice and complying with government regulations. Thus, notice and compliance costs are likely not covered by errors and omissions policies with respect to privacy claims, even if the insured can obtain reimbursement of litigation expenses.[144]

Some insurers leave scope of coverage defined in general terms or leave terms with respect to "covered privacy breach" or "private information" virtually undefined.[145] Some

---

[142] Robert Paul Norman, *Virtual Insurance Risks*, 31 THE BRIEF 14 (2001).

[143] Robert H. Jerry, II and Michele L. Mekel, *Cybercoverage for Cyber-Risks: An Overview of Insurers' Responses to the Perils of E-Commerce*, 8 CONN. INS. L.J. 7 (2001).

[144] Nancy D. Adams et al., *Cloud Cover: Insuring Technology & Cyberliability Risks*, ABA SEC. OF LIT. 2012 INS. COVERAGE LIT. COMM. (Oct. 18, 2012).

[145] SIEMENS AND BECK ON OBTAINING OPTIMAL CYBER INSURANCE, 2012 Emerging Issues 6613 (2012).

insurers define scope of coverage by defining terms with reference to specific lists of statutes or regulations that must be breached, or specific combinations of information that must be disclosed, to trigger coverage.[146] This has the effect of potentially resulting in artificial coverage gaps unless policy language is drafted carefully.

C. Other Considerations

There is a general lack of standardization of cyber insurance policy forms, leading to unpredictable scope of coverage across different insurance companies. Because there is a lack of standardization in policy language, an entity seeking insurance coverage should consider what exposures it wants covered. It must also understand the distinctions between "first party," "second party," and "third party" liability and coverage.

IV. Other Policies

A. First-Party All Risk Insurance

First-party all risk insurance may cover physical injury to or loss of use of servers, hard drives, or other insured hardware.[147] It may cover damage arising from cyber-attacks that is not expressly excluded in the policy. However, some courts do not consider "physical damage" to include compromised computer data.[148]

B. Business Interruption Coverage

Business interruption coverage insurance is intended to reimburse the insured for loss due to business interruption. Coverage may extend to extra expenses and lost profits associated with

---

[146] *Id.*

[147] *See, e.g., Lambrecht & Assocs., Inc. v. State Farm Lloyds*, 119 S.W.3d 16, 25 (Tex. App. 2003) (finding coverage where virus rendered business server useless).

[148] *See, e.g., Ward Gen. Ins. Servs., Inc. v. Employ'rs Fire Ins. Co.*, 7 Cal. Rptr. 3d 844 (Cal. Ct. App. 2003) (finding computer information too intangible to be subject to direct physical loss).

cyber liability. The policy may also cover computer network interruptions.[149] If an organization suffers loss to business income or incurs extra expenses due to computer network unavailability to engage in e-commerce (or if data lost or corrupted), it may seek coverage for those losses via business interruption coverage.[150]

C. Commercial Crime Insurance

Commercial crime insurance policies are designed to protect organizations from loss of money, inventory, or other assets (such as data) resulting from crime. Policies may have endorsements that expressly cover data breaches or other claims with respect to computer fraud or computer theft. For example, the policy may cover hacking and theft of consumer data. Cyber liability may be covered under commercial crime insurance policies. However, there may be limitations, such as exclusions for indirect or consequential losses of any kind and loss of "future" income, thus limiting the insured's ability to recover its own losses.[151] Additionally, intent is required and commercial crime insurance policies are generally limited to money, securities, and tangible property

D. Directors and Officers

Directors and officers policies typically provide coverage for losses suffered by individual directors or officers and also covers losses suffered by the company for certain

---

[149] *See, e.g., Southeast Mental Health Ctr., Inc. v. Pac. Ins. Co.*, 439 F. Supp. 2d 831 (W.D. Tenn. 2006) (finding coverage for business interruption due to corruption of insured's computer system).

[150] SIEMENS AND BECK ON OBTAINING OPTIMAL CYBER INSURANCE, 2012 Emerging Issues 6613 (2012).

[151] Nancy D. Adams et al., *Cloud Cover: Insuring Technology & Cyberliability Risks*, ABA SEC. OF LIT. 2012 INS. COVERAGE LIT. COMM. (Oct. 18, 2012)..

claims.[152] Such policies may cover securities lawsuits raising claims that a company and its management failed to take sufficient steps to mitigate cyber risks or inadequately reported cyber exposures. They may cover privacy and data security claims that seek economic damages when such claims are not excluded by the policy. However, directors and officers policies are usually only for specific third-party claims and may exclude professional services or privacy losses.

E. "New" Coverage Options[153]

There are also many fairly new types of coverage that may apply to the cyber insurance context. One of these new types of coverage is network security liability. This type of coverage addresses liability to a third party resulting from the following situations: (1) failure of network security to protect against destruction, deletion, or corruption of a third party's electronic data; (2) denial of service attacks against internet sites or computers; and (3) transmission of viruses to third-party computers and systems. Media liability covers specified perils arising from online or print media and advertising content. Privacy liability covers liability to a third party resulting from disclosure of confidential information collected or handled by the insured or under the insured's care, custody or control. This includes coverage for vicarious liability, such as where a vendor loses information the insured had entrusted to them in the normal course of the insured's business. Additionally, insurers may offer crisis management and identity theft response funds. Such funds may cover expenses to comply with privacy regulations (*e.g.*, communication to and credit monitoring services for affected customers). These funds also cover expenses incurred in

---

[152] SIEMENS AND BECK ON OBTAINING OPTIMAL CYBER INSURANCE, 2012 Emerging Issues 6613 (2012).

[153] Nancy D. Adams et al., *Cloud Cover: Insuring Technology & Cyberliability Risks*, ABA SEC. OF LIT. 2012 INS. COVERAGE LIT. COMM. (Oct. 18, 2012).

retaining a crisis management firm for a forensic investigation or for protecting/restoring your reputation as a result of the actual or alleged violation of privacy regulations.

Also, there are cyber extortion policies to cover the following situations: (1) ransom or investigative expenses associated with a threat directed at an insured to release, divulge, disseminate, destroy, steal, or use confidential information taken from the insured; (2) ransom or investigative expenses associated with a direct threat at the insured to introduce malicious code into your computer system, corrupt, damage, or destroy your computer system; (3) ransom or investigative expenses associated with a direct threat at the insured to restrict or hinder access to the insured's computer system. These new coverage options may also include network business interruption, which covers reimbursement of loss of income and/or extra expense resulting from an interruption or suspension of computer systems due to a technology failure. Included in network business interruption coverage is sub-limited coverage for dependent business interruption. Insurers may also offer data asset protection, which covers the recovery of costs and expenses you incur to restore, recreate, or recollect your data and other intangible assets (*e.g.*, software) that are corrupted or destroyed via computer attack.

It is important to note that, although these "new" coverage options were designed to apply specifically to cyber liability issues, these "new" coverage options may still be subject to certain exclusions. Examples of exclusions that may apply to these "new" coverage options include, among other things, failure to maintain or upgrade security, errors and omissions, and war and terrorism. Because of the lack of standardization with respect to these "new" coverage options, it is important for policyholders to understand and identify potential exceptions to coverage and seek and obtain coverage options most favorable to their specific situations.

V. HIPAA Violations and Cyber Insurance

Healthcare-related security breaches present unique insurance coverage issues. In 2013, the U.S. Department of Health and Human Services announced important modifications to the Health Insurance Portability and Accountability Act's ("HIPAA") Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health ("HITECH") Act and the Genetic Information Nondiscrimination Act ("GINA").[154] These changes are known as the Omnibus Rule.

A. Potential Liability for HIPAA Violations Has Recently Expanded

Under the HIPAA Omnibus Rule, "breach" has been more broadly defined. Previously, a breach required a finding that the access, use or disclosure of personal health information posed "a significant risk of financial, reputational or other harm to an individual."[155] This harm threshold had to be met before health care providers were required to notify patients of the breach. The Omnibus Rule replaced the "harm threshold" with a new standard.[156] Under the new regulations, a breach is presumed whenever protected health information is acquired, accessed, used or disclosed in a way that violates HIPAA's stringent standards. Patients must be notified unless a risk assessment demonstrates that there is a "low probability that the protected health information has been compromised."[157]

---

[154] Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act, 78 Fed. Reg. 5566 (Jan. 25, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

[155] *Id.* at 5639.

[156] *Id.* at 5566.

[157] *Id.* at 5641.

At the same time, penalties for HIPAA violations have increased. The maximum penalty is now $1.5 million annually for all violations of an identical provision.[158] However, as the U.S. Department of Human Health Services warns, "a covered entity or business associate may be liable for multiple violations of multiple requirements, and a violation of each requirement may be counted separately. As such, one covered entity or business associate may be subject to multiple violations of up to a $1.5 million cap for each violation, which would result in a total penalty above $1.5 million."[159]

Meanwhile, as penalties for HIPAA violations have expanded, affirmative defenses for these violations have narrowed. The Omnibus Rule removes the previous affirmative defense to the imposition of penalties if the covered entity did not know and with the exercise of reasonable diligence would not have known of the violation.[160] Moreover, previously there were no penalties for violations that were timely corrected unless the violation was due to willful neglect. However, under the Omnibus Rule, penalties may now be imposed even for violations that are timely corrected.[161]

The Omnibus Rule not only affects health care providers, but makes business associates of these entities directly liable for compliance with many of the HIPAA Privacy and Security Rules' requirements. The Omnibus Rule defines "business associate" as a person or entity "'who creates, receives, *maintains*, or transmits' (emphasis added) protected health information on

---

[158] *Id.*

[159] *Id.* at 5584.

[160] *Id.* at 5585.

[161] *Id.* at 5586.

behalf of a covered entity."[162] Moreover, now "subcontractors"—persons "to whom a business associate delegates a function, activity, or service"—are specifically included in the new definition of "business associate."[163] The rules are not simply limited to direct subcontractors, but also apply to "downstream entities."[164]

Health providers may now be liable for violations by business associates and subcontractors. The new Omnibus Rule could increase the likelihood that hospitals and other health care providers will face liability for conduct by business partners. This is significant, as by some estimates these business partners, rather than the health care providers themselves, are responsible for more than 60% of HIPAA violations.[165] The Omnibus Rule could potentially increase the possibility of liability by health care providers for the actions of third parties.

B. Insurance Coverage for HIPAA Violations

Given the addition of new regulations under HIPAA, an increase in fines and penalties for HIPAA violations, and the possibility of broader liability for the acts of business partners under the Omnibus Rule, it is essential that health care providers and business associates protect themselves against potential risk exposure. Federal enforcement of HIPAA claims against health care providers is on the rise. Insurance is an important means of protecting against these claims, as well as from fines and penalties if liability is found.

Traditional D&O and E&O policies may provide coverage for HIPAA violations unless explicitly excluded. For example, even under policies that do not have express penalty coverage,

---

[162] *Id.* at 5572.

[163] *Id.* at 5573.

[164] *Id.*

[165] HIPAA Compliance, http://www.hipaa.co/hipaa-compliance (last visited Mar. 18, 2013).

HIPAA violations still may be covered.[166] Moreover, it may be possible to obtain coverage for business associates and subcontractors as "independent contractors" insured under a traditional policy. At least one court has rejected an insurer's attempt to narrowly construe independent contractor language in a healthcare D&O policy.[167] However, recently many insurance companies have developed health care policies that provide coverage specifically for HIPAA investigations. These policies cover defense costs and penalties associated with HIPAA violations.

Certain insurers provide coverage specifically for losses associated with HIPAA violations. For example:

> "**Loss**" means damages, judgments (including pre/post-judgment interest on a covered judgment), settlements and Defense Costs; however, Loss shall not include:
>
> (1) civil or criminal fines or penalties imposed by law, **except**:
>
> (ii) HIPAA Penalties, subject to the HIPAA Penalties Sublimit of Liability set forth under Clause 6 "LIMIT OF LIABILITY (FOR ALL LOSS – INCLUDING DEFENSE COSTS)" of this policy.

---

[166] For example, on January 6, 2012, San Francisco Superior Court Judge Howard Kahn ruled that under the California Invasion of Privacy Act, statutory damages were not "fines, . . . sanctions or penalties" but rather covered "damages," holding they represent a form of "statutory liquidated damages" set by the legislature in circumstances where the actual damages from a breach event are difficult to measure. *Visa Inc. v. Certain Underwriters at Lloyd's, London*, Case No. CGC-11-509839 (Jan. 6, 2012).

[167] On January 15, 2013, Santa Barbara Superior Court Judge Thomas Anderle rejected an insurer's argument that doctors could not be "independent contractors" because they were not under the "exclusive direction" of the hospital. The Court held that the definition of "independent contractor" as being under the "exclusive direction" of the hospital was ambiguous, and denied the insurer's motion for summary judgment. *Cottage Health System v. Travelers Cas. & Sur. Co.*, Case No. 13821220 (Jan. 15, 2013). The authors of this article represented the insured hospital in this case.

In this particular example, "Wrongful Act" was defined as "the failure to comply with the privacy provisions of HIPAA." Likewise, "HIPAA Penalties" included "civil money penalties imposed upon an Insured for violation of the privacy provisions of the Health Insurance Portability and Accountability Act of 1996 and any amendments thereto."[168]

Certain policies provide coverage explicitly for HIPAA investigations:

> "**HIPAA Proceeding**" means an administrative proceeding, including a complaint, investigation or hearing instituted against you by the Department of Health and Human Services or its designee alleging a violation of responsibilities or duties imposed upon you under the Health Insurance Portability and Accountability Act ("HIPAA"), or any rules or regulations promulgated thereunder, with respect to the management of confidential health information.[169]

In this particular policy, the insuring agreement broadly provided express coverage for all "claims expenses" related to any "HIPAA Proceeding." Because not only the fines associated with HIPAA violations, but defending against the investigations themselves can be quite costly, investigations coverage is necessary.

Given potential liability created by business associates' and subcontractors' activities under the new Omnibus Rule, health care providers should make sure that their policies cover the exposures of others. Where possible, health care providers should add business associates and subcontractors to their list of additional insureds. Moreover, hospitals should enter into agreements with their business associates and subcontractors whereby the latter would be responsible for obtaining additional insured coverage for the hospital under their own policies.

---

[168] Chartis Insurance, http://www.chartisinsurance.com/ncglobalweb/internet/US/en/files/AIG%20Executive%20Liability-%209.99%20Amendatory%20Endorsement%205-28-08_tcm295-92662.pdf (last viewed Mar. 18, 2013).

[169] *Id.*

In certain circumstances, healthcare providers may also want to consider purchasing a cyber liability policy that insures against liability for data security breaches, including protected health information under HIPAA.

VI. Cyber Insurance Options

A. Traditional Policies May Not Provide Right Type of Coverage

Although nearly every company has a potential cyber risk, not every company has the right coverage. Too often, companies still rely on traditional policies to provide coverage and that is not a safe bet.

Cyber attacks often result in the corruption of electronic data. However, property coverage many not respond to that loss because many jurisdictions require injury to be tangible property, a threshold that damage to electronic data generally does not meet. In addition, general liability policies will not respond when the injury results from an intentional act. Many data breaches and network attacks involve hackers or other criminal actors who maliciously attempt fraud, theft or disruption of networks. Insureds may seek coverage for advertising injury, but that usually requires publication and lost data is often not seen by anyone. Still, whether a general liability policy provides coverage for these risks depends on the individual policies and the nature of the particular harms. As a result, coverage disputes remain common.

Insureds may run into similar problems seeking coverage under errors and omissions policies. A typical professional liability policy responds when an insured intentionally carries out a service for a customer, but commits an error when doing so. If a company's professional services involve handling data or other technology-related activity, its E&O policy will more likely cover a loss resulting from an information technology failure. However, the insurer will not cover wrongful acts that lie outside of the activity that was intended to be covered.

In addition, a standard E&O policy might provide some coverage for issues surrounding security failures during online contacts with third-parties, However, a typical data breach scenario involves either first-party losses or "pre-claim" activities like providing notice to parties at risk, performing credit monitoring and otherwise complying with government regulations. Although an insured may be able to obtain reimbursement of litigation expenses, notice and compliance costs are likely not within the coverage of a typical professional liability policy. More importantly, other pre-claim expenses typically contemplated under a network security and privacy policy such as costs to conduct a forensic investigation and costs to retain a public relations firm will not be covered under a standard E&O policy.

In some instances, insureds may avail themselves to their commercial crime policies. However, those may also limit coverage for a cyber event by excluding indirect or consequential loss of any kind, as well as the loss of "future" income. That may serve to deny consequential loss caused by the theft of confidential information, which drives much of the costs and litigation arising from cyber incidents.

The Sixth Circuit recently addressed this latter exclusion, holding that there was coverage for first-party and third-party losses arising from the theft of customer credit card information by hackers under a crime policy's computer fraud endorsement.[170] The court found that the crime policy covered third-party liability losses because the underlying fraud "result[ed] directly from" the theft of the insured's property by computer fraud. The court also denied any application of an exclusion barring coverage for "any loss of proprietary information, Trade Secrets, Confidential Processing Methods or other confidential information of any kind" because credit

[170] *See DSW Inc. v. National Union Fire Ins. Co. of Pittsburgh, Pa.*, Case No. 10-4576/5608 (Aug. 23, 2012).

card information was not the type of confidential information envisioned by the exclusion. Otherwise, the exclusion would vitiate the coverage that the policy promised to provide. Although the court found that this particular claim was covered, the decision further emphasizes the importance of reading the insuring agreements and exclusions of each policy carefully.

B. Data Breach Coverage Provides Key Protection For Third-Party and First-Party Losses

The most prominent problem against which a cyber liability policy aims to protect is the data breach, where a malicious hacker or a negligent employee puts either company or customer information at risk. A recent study of data breaches analyzing claim payouts concluded that the average loss is $3.7 million per data breach event, a number that does not include the first party expenses of the organization that suffered the breach. Although a data breach can involve loss of customer data, company data (such as intellectual property), or employee data, the risks for which cyber risk policies can provide coverage often include other types of cyber-related events. For example, another common problem is an organization receiving a computer virus, or passing along the same to a customer or other third-party, which itself can cause a loss of data or an inability to use computer systems. Unfortunately, overzealous or rogue employees also are a source of risk, and they can cause trouble by slandering a competitor via social media, gaining access to another company's electronically-stored information, or infringing on copyrighted materials.

An organization facing a data breach, or any other type of cyber risk, is likely to incur multiples types of damages. In the event of lost third-party data, nearly all states now have regulations governing how a company must provide notice to its customers (hence, the letters we receive all too frequently informing consumers that personal information may be at risk), as well as the possibility of penalties for failing to protect data. Almost inevitably, there will be

lawsuits, with the substantial costs that those entail. If the company's own data is at risk – through a data breach or malware attack – the organization will need to take steps to replace or protect its data and often will suffer losses associated with an interruption to its business. In other words, cyber risks can entail significant first- and third-party losses.

When a third party is involved, a company may be faced with a substantial exposure. Where previously plaintiffs had to prove actual harm or damages to establish standing, courts have begun to consider data breach litigation in the same light as toxic tort litigation. In other words, the threat of a future injury (identity theft) might be enough to establish damages, just as the threat of a future medical condition in a toxic tort case is sufficient to establish damages (*i.e*., asbestos). *Anderson v. Hannaford Bros.*, No. 10-2384 and No. 10-2450 (1st Cir., Oct. 20, 2011) (court reinstated negligence and implied contract claims brought on behalf of plaintiffs whose financial data was compromised based on the theory that it was reasonably foreseeable that plaintiffs whose personal information was misused would have to take action to protect themselves); *Pisciotta v. Old National Bancorp,* 499 F.3rd 629 (7th Cir. 2007); *Krottner v. Starbucks Corp*., 628 F.3rd 1139 (9th Cir. 2010). However, a recent federal court decision changed this threshold significantly by highlighting how difficult it may be for a plaintiff to articulate that he or she has suffered an "injury" – as defined by Article III of the US Constitution - as a result of a data breach. On September 3, 2013, the US District Court for the Northern District of Illinois dismissed a class-action complaint (*in re Barnes & Noble Pin Pad Litigation)* arising from a credit card "skimming" attack against Barnes & Noble. The court held that plaintiffs failed to demonstrate standing under Article III and therefore could not proceed with their complaint for breach of contract, violation of the Illinois Consumer Fraud and

Deceptive Practices Act, invasion of privacy, violation of the California Security Breach Notification Act and violation of the California Unfair Competition Act.

The retailer moved to dismiss the complaint for lack of standing and the court agreed. Applying the rationale in the Supreme Court's decision in *Clapper v. Amnesty International*, the court explained that to establish standing under *Clapper*, a plaintiff must demonstrate that he or she has suffered an "injury in fact" that is "certainly impending." The potential for future injury, as alleged against the retailer, failed to meet this test, the court said. This opinion was significant as it suggests that data breach litigation post *Clapper* will be more likely to be decided on standing grounds and that speculation of future harm will not suffice. Given the ever evolving and constantly changing legal and regulatory landscape, insureds should be clear in understanding the coverage their policy affords in terms of regulatory fines and penalties for failure to comply with the applicable regulations governing their industry. In addition, cause does not matter. Since a regulatory action usually precedes a civil action, substantial legal and forensic investigation costs can be incurred even for events where no one is harmed or even at risk. For companies processing credit card data, compliance with the PCI standards definitely helps to drive security but will not necessarily defeat a claim for negligence. As a result, any claim involving third parties can be extremely expensive and time-consuming to resolve.

C. Coverage Is Becoming More Common But There Is No Standard Policy Language

In light of the uncertainty of whether the typical menu of available coverage will cover losses from cyber risks, demand for insurance policies specifically designed for these events continues to grow. This demand has increased with the SEC Division of Corporate Finance's Disclosure Guidance on Cybersecurity, issued on October 13, 2011. The Disclosure Guidance recommended that companies should disclose the risk of cyber incidents for their particular

business, as well as what steps the company takes to address those risks, including a description of the relevant insurance coverage. While not creating an official requirement to purchase cyber liability insurance, after the SEC specifically identified this as a concern, more companies demonstrated an increasing awareness of the issue, including the litigation risks if they are not properly insured. The SEC Disclosure Guidance raises the question of whether the failure to purchase cyber liability insurance can open a company up to D&O claims for breach of fiduciary duty or securities violations for not adequately protecting the company against such risks if a cyber liability event occurs, or for not disclosing to shareholders knowledge of inadequate protections or ongoing risks. According to a recent study, nearly 85% of Board members acknowledged familiarity with basic Information Security standards such as ISO 27001/2 however, only 35% knew where their organization stood as regards complying with basic information security standards. According to the *Wall Street Journal,* in the first six months of 2013, there were over 800 regulatory filings that mentioned cyber related risks. This represents a 106% increase from the same time last year, thus evidencing the increasing awareness of identifying cybersecurity risks.

Even though some of these issues are still relatively new, the risks are well-known and there are now a number of examples where insurers have provided substantial coverage for these types of losses. For example, carriers have covered claims where hackers have stolen credit card information and passwords. Carriers have also covered claims involving employees where records were stolen and sold or where the employee misappropriated confidential information from a competitor. Coverage has also been found where the insured simply lost or accidentally published confidential information.

Although specific cyber liability policies – or endorsements to GL or E&O policies addressing these risks – have been available for a few years, they have historically been inconsistent, without the standardization that is typical of policy forms in some more well-established areas. Positively, this has begun to change. Typically these policies provide for third-party cyber liability coverage that may include protection against liability for permitting access to identifying information of customers (including information stored by third parties on your behalf), transmitting a computer virus or malware to a third-party customer or business partner, or failing to notify a third party of their rights under the relevant regulations in the event of a security breach. Such policies also can cover "advertising injury"-like harms through the use of electronic media, such as unauthorized use or infringement of copyrighted material, as well as libel, slander, and defamation claims. First-party cyber liability coverage typically includes paying for the costs of providing notice and credit monitoring to individuals whose identifying information was compromised; the costs associated with the hiring of a forensic investigation to determine the scope of the breach and taking steps to stop the breach; obtaining public relations services to counteract the negative publicity that can be associated with a data breach or other cyber risk losses; reimbursing the costs of responding to government investigations; and reimbursing the costs of replacing damaged hardware or software and replacing data. In addition, some companies offer coverage for relevant regulatory fines and penalties as well as Payment Card Industry ("PCI") fines and penalties (where insurable by law), reimbursement for damages to the insured entity caused by computer fraud; reimbursement for payments made to parties blackmailing the company or the costs of responding to parties vandalizing the company's electronic data; as well as network interruption costs and contingent network interruption which provide for reimbursement of your own loss of income and/or extra

expense resulting from your vendor's interruption or suspension of systems due to a failure of technology which causes a system outage.

In the absence of transferring risk through insurance, several risk mitigation techniques must be considered. First, insureds would be wise to make sure that there are provisions for defense and indemnification should your vendor be the cause of damage to your client and further ensure, there are sufficient limitations of liability with such vendor in place. Additionally, maintenance of a privacy policy to ensure your legal department is kept current with respect to relevant regulatory requirements and disclosure as well as privacy law. Third, maintaining a business continuity plan is an integral part of surviving a data breach, but annual testing must be conducted. Fourth, conduct full background checks of employees as part of the hiring process and provide privacy awareness training to employees. As companies can never be too secure, they may also want access to data to be contingent on an employee's role and updated semi-annually; enforce a strong password management process; ensure mobile devices are secure; use a data segregation scheme and remove old data and finally and most importantly, in the absence of risk transfer through insurance, maintain an agreement with a reputational risk advisor.