AN A.S. PRATT PUBLICATION
JANUARY 2016
VOL. 2 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 2 | NUMBER 1 | JANUARY 2016

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3000
Fax Number .... (518) 487-3584
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3000

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [3] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2016–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Danger in the Wires: Insurance Coverage for Cyber Risks

By John L. Watkins*

The author of this article discusses insurance coverage for cyber risks and recommends that businesses assess their risks carefully, and try to ensure their coverage options are tailored to meet those risks.

Cyber risks are everywhere. One only has to browse the web, turn on the television, or (for true Luddites) open a newspaper to learn of the latest hack, data breach, or electronic invasion of privacy. A national retailer reported that *40 million* debit and credit cards were affected in a breach occurring during a three-week period in late 2013.[1] More recently, the federal government admitted that it experienced a huge breach affecting over 20 million individuals, including Social Security numbers and highly sensitive information. Astonishingly, "hackers obtained information from the *security clearance applications*—known as SF-86's—of *19.7 million people*."[2]

Many small and medium-sized businesses probably conclude, however, that they are too small to be tempting targets. Unfortunately, this is wishful thinking. The Ponemon Institute has surveyed the cost of data breaches for a number of years. In its report published in May 2015, Ponemon reported on the study of 62 organizations with data breaches ranging from 5,000 to slightly less than 100,000 compromised records. The study purposefully excluded breaches of more than 100,000 records in order to be more representative of typical breaches: "The average cost of a data breach in our research does not apply to catastrophic or mega data breaches because these are not typical of the breaches most organizations experience."[3] Ponemon found that the average total cost of a data breach in the companies studied was $6.53 million.[4]

---

* John L. Watkins is a partner in Thompson Hine LLP's Business Litigation and Corporate Transactions & Securities groups and a member of the International practice. He focuses on insurance issues and teaches insurance law as an adjunct professor at the University of Georgia School of Law. He may be contacted at john.watkins@thompsonhine.com.

[1] http://www.forbes.com/sites/kellyclay/2013/12/18/millions-of-target-customers-likely-affected-by-data-breach (last visited on July 10, 2015).

[2] http://www.cnn.com/2015/07/09/politics/office-of-personnel-management-data-breach-20-million (last visited on July 10, 2015) (emphasis added).

[3] Poneman Institute LLC, *2015 Cost of Data Breach Study*, p. 4 (available for download at http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03055usen/SEW03055USEN.PDF) (last visited on July 10, 2015) (cited hereinafter as "Ponemon").

[4] Ponemon, p. 1.

TYPES OF LOSSES

Cyber losses involve more than just data breaches, and may involve what is known in the insurance world as a "first party" loss or a "third party" loss. A first party loss is one experienced by the insured—a common example would be a fire loss under a property insurance policy. A third party loss is one in which a third party asserts a claim against the insured—a common example would be when a person injured in an accident makes a claim against the insured, which is in turn covered by the insured's liability policy. Cyber losses may involve a large variety of first party or third party losses and particular incidents may involve both. Examples include:

- A malicious attack involving computer viruses, malware or spyware may result in damages to the insured's computer system, loss of data, or both, resulting in corresponding downtime and loss of revenue, which would be first party loss.
- The same attack may result in denial of service or loss of data by the insured's customers who rely on the insured's computer system, which may cause the insured's customers to assert claims against the insured, which would be third party claims.
- Other third party claims may result from exposure of the customers' private data.

DOES REGULAR BUSINESS INSURANCE COVER THAT?

Companies facing data breaches or other cyber-related losses have had some success in seeking coverage under their traditional commercial property and commercial general liability ("CGL") insurance. The results, however, have been at best mixed. Further, insurers are actively attempting to avoid coverage for cyber losses under traditional policies, and such policies are being endorsed to exclude potential coverage for cyber losses.

Commercial Property Insurance

Insureds have had some success seeking coverage for cyber-related losses under commercial property insurance. Under a policy insuring "[a]ll Risks of direct physical loss or damage from any cause," a federal district court concluded that the temporary loss of functionality of computers resulting from a loss of custom settings due to a power outage was covered. The court found that physical damage "is not restricted to

the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality."[5] This reasoning was, however, rejected by another district court.[6]

In *NMS Servs. v. The Hartford*,[7] the court found coverage under a business interruption policy that covered lost business income due to a suspension in operations "caused by direct physical loss of or damage to property at the described premises . . ." The insured sustained a loss of data necessary for its operations caused by an employee installing two hacking programs that enabled him to access the computers and destroy the data remotely. After the employee was fired, he used the programs to gain access to the insured's programs and destroy the data. The court found that there "is no question that NMS suffered damage to its property, specifically, damage to the computers it owned . . . ."[8]

Although these cases are potentially helpful to insureds, there is very little authority on this question, and there is case law to the contrary.[9] As shown below, the results under CGL policies for third party liability claims for "property damage" are also mixed. Further, ISO has issued forms that some insurers may use that effectively restrict coverage, including through the use of "additional coverage" for electronic data with a presumptively inadequate sublimit of $2,500.[10]

Commercial General Liability Insurance

Most businesses will have a CGL policy as the mainstay of their liability insurance program. CGL policies tend to be fairly uniform in their policy terms—although there can be important differences—and are typically written on policy forms from the Insurance Services Office ("ISO"). The basic coverages offered under a CGL policy are Coverage A, for damages because of "bodily injury" and "property damage," and Coverage B for damages because of "personal and advertising injury."

Before turning to specific issues regarding cyber-related claims, two advantageous characteristics of CGL coverage should be noted: First, both Coverage A and Coverage B include a defense obligation, typically meaning that the insurer has the "right and duty to defend" any "suit" to which the insurance may apply. This means the insurer

---

[5] *American Guar. & Liab. Ins. Co. v. Ingram Micro, Inc.*, 2000 U.S. Dist. LEXIS 7299, *6 (D. Ariz. Apr. 18, 2000).

[6] *Am. Online, Inc. v. St. Paul Mercury Ins. Co.*, 207 F. Supp. 2d 459, 469-470 (E.D. Va. 2002) (CGL policy). The court did, however, find "property damage" under the alternative definition in the CGL policy, but then found coverage barred by an exclusion.

[7] 62 Fed. Appx. 511, 512 (4th Cir. 2003).

[8] 62 Fed. Appx. at 514.

[9] *E.g., Ward General Ins. Services, Inc. v. Employers Fire Ins. Co.*, 7 Cal. Rptr. 3d 844, 851, 114 Cal. App. 4th 548, 556 (Cal. App. 4th Dist. 2003).

[10] ISO Form CP 00 99 06 07 (2007) p.6 (providing "additional coverage" for "electronic data" and containing sublimit).

must appoint and pay for legal counsel to defend any lawsuit against the insured making a claim that is *potentially* covered by the policy.[11] Further, in most CGL policies, the defense costs do not erode (reduce) the policy limits available to pay claims.[12] In contrast, defense costs in most cyber policies do erode the policy limits.

Second, CGL policies are usually "occurrence" based policies. This means that they cover claims and lawsuits that arise from "occurrences" (events) that happen during the policy period, or, in the case of personal and advertising injury, "offenses" that happen during the policy period. Under an "occurrence" policy, it does not matter when the claim is made or the lawsuit is filed, even if years later. Most cyber policies, on the other hand, are "claims made" policies that contain important limitations discussed below.

Coverage A: Bodily Injury and Property Damage

Coverage A of a CGL policy typically provides that the insurer will pay damages the insured is legally obligated to pay "because of 'bodily injury' or 'property damage' to which this insurance applies."[13] The question thus becomes whether cyber-related liabilities result in damages "because of 'bodily injury' or 'property damage.' "

"Bodily injury" is defined to mean "bodily injury, sickness or disease sustained by a person, including death resulting from any of these at any time."[14] A plaintiff could certainly allege in a data breach claim that the exposure of private information resulted in severe emotional distress, perhaps accompanied by resulting physical symptoms. Some have suggested that such allegations may trigger coverage for "bodily injury," at least for purposes of providing a defense.[15] The majority rule appears to be that claims alleging purely emotional injury are not covered, although the result may differ in some jurisdictions if it is alleged that the emotional injury included physical 5manifestations.[16] Although claims alleging emotional injury (particularly if

---

[11] J. Watkins, *Georgia Business Litigation 2016*, Chapter 12, Insurance Law, at 565-566 (ALM 2015) (R. Port Ed.).

[12] *Id.* at 538-539 (2016).

[13] ISO Form CG 00 01 04 13, p. 1 (2012).

[14] ISO Form CG 00 01 04 13, p. 13 (2012).

[15] S. Godes and J. Smith, *Insurance for Cyber Risks: Coverage Under CGL and "Cyber" Policies*, ABA Section of Litigation, 2012 Insurance Coverage Litigation Committee CLE Seminar, March 1-3, 2012, p. 4, *available at* http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2012_inscle_materials/17_1_risks.authcheckdam.pdf (last visited August 17, 2015). The defense obligation is generally understood to be broader than the duty to pay settlements or judgments.

[16] *50-State Survey: Is Emotional Injury "Bodily Injury"?*, 1-11 General Liability Insurance Coverage § 11.01; B. Ostrager and T. Newman, *Handbook on Insurance Coverage Disputes*, Vol. 1, § 7.03(a) at 397 (13th ed. 2006) ("Ostrager"). The result changes in some jurisdictions if the claim alleges physical manifestations resulting from emotional harm. Ostrager at 399-401. *See also*, Ostrager at 403-412 (containing 50 state survey).

accompanied by physical manifestations) might be covered in some jurisdictions, there appears to be a dearth of case law on coverage for such claims resulting from data breaches.

There are other cyber-related situations in which coverage for "bodily injury" may potentially apply, such as if a hacker disabled life safety systems in a building, resulting in injuries or even loss of life. *Wired* recently reported that hackers, fortunately in a demonstration, were able to gain remote control of a late-model Jeep Cherokee even to the point of disabling the car's transmission and brakes.[17] It is not a far stretch to envision claims alleging bodily injury or death from such episodes would be covered under Coverage A or under an automobile liability policy.

"Property damage" in a typical CGL policy is defined to mean (a) "Physical injury to tangible property, including all resulting loss of use of that property," or (b) "Loss of use of tangible property that is not physically inured." The definition further states that "For the purposes of this insurance, electronic data is not tangible property," and 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 and floppy disks, CD-ROMs, tapes, drives, . . . or any other media which are used with electronically controlled equipment."[18]

Despite the exclusion of "electronic data" from the definition of "property damage," insureds have had some success in seeking coverage. The Eighth Circuit recently found coverage in a case alleging that the defendant's web-based advertising services had caused the claimant's computer to be "taken over and could not operate," to freeze up, and to stop running or operate so slowly that it would in essence become inoperable. The court found there was coverage under the second part of the "property damage" definition for "loss of *use* of tangible property that is not physically injured."[19]

It is certainly possible to envision other circumstances in which a cyber event could lead to loss of tangible property, or, alternatively, loss of use of tangible property that is not physically injured. For instance, if an attack resulted in a loss of electrical power causing food or medicines to spoil, that would constitute a loss of tangible property.

---

[17] A. Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me In It*, Wired (July 21, 2015), *available at* http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (last visited on August 17, 2015).

[18] ISO Form CG 00 01 04 13, pp. 15-16 (2012).

[19] *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797, 802 (8th Cir. 2010) ("The plain meaning of tangible property includes computers, and the Sefton complaint alleges repeatedly the 'loss of use' of his computer. We conclude that the allegations are within the scope of the General Liability policy"). *See also*, *Am. Online, Inc. v. St. Paul Mercury Ins. Co.*, 207 F. Supp. 2d 459, 470 (E.D. Va. 2002) (finding loss of use of tangible property when complaint alleged that AOL caused loss of use of computers and computer functionality, but concluding no coverage existed because allegations were otherwise excluded), *aff'd*, 347 F.3d 89 (4th Cir. 2003); *State Auto Prop. & Cas. Ins. Co. v. Midwest Computers & More*, 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001) ("Because a computer clearly is tangible property, an alleged loss of use of computers constitutes 'property damage' within the meaning of plaintiff's policy," but finding coverage subject to an exclusion).

Similarly, a vehicle rendered inoperable by an attack would seem to fit squarely within the definition of loss of use of tangible property that is not physically injured.[20]

Coverage B: Personal and Advertising Injury

Insureds have also had some success seeking coverage for data breaches under Coverage B, which typically provides that the insurer "will pay those sums that the insured becomes legally obligated to pay because of 'personal and advertising injury'. . ."[21] "Personal and advertising injury" is defined to mean injury, including consequential bodily injury, arising out of certain enumerated "offenses." In the cyber context, the most important "offense" has been: "e. Oral or written publication, in any manner, of material that violates a person's right of privacy."

Insureds have sometimes obtained coverage for data breaches under Coverage B for the violation of the "right of privacy" offense.[22] Insureds have also had some success in obtaining coverage under this provision for claims involving the unwanted receipt of electronic communications, including unsolicited faxes, telephone calls and spam email.[23] Some courts have distinguished between violations of privacy involving the

---

[20] A commentator has suggested that customers denied the use of their credit cards by a cyber attack would sustain loss of use of tangible property (their credit cards) not physically injured. S. Godes, *Should Retailers Rely On CGL Coverage For Data Breaches?*, Law 360, March 12, 2015, *available at* http://www.law360.com/insurance/articles/630136 (last visited August 17, 2015).

[21] ISO Form CG 00 01 04 13, p. 6 (2012).

[22] *Travelers Indem. Co. of Am. v. Portal Healthcare Solutions, LLC*, 35 F. Supp. 3d 765, 771-772 (E.D. Va. 2014) (finding duty to defend under policies providing coverage for "electronic publication of material that . . . gives unreasonable publicity to a person's private life" or "electronic publication of material that . . . discloses information about a person's private life" when defendant allegedly provided access to underlying plaintiffs' medical records on the Internet; finding making records available to public satisfied "publication" requirement); *Tamm v. Hartford Fire Ins. Co.*, 2003 Mass. Super. LEXIS 214, *11, 16 Mass. L. Rep. 535 (Mass. Super. Ct. 2003) (allegations that insured consultant accessed email accounts of former customer and its executives and sent them to former customer's outside counsel "satisfies both prongs under the invasion of privacy clause of the policy"; finding that transmission to former customer's own counsel satisfied "publication" requirement).

[23] *E.g.*, *Valley Forge Ins. Co. v. Swiderski Elecs., Inc.*, 223 Ill. 2d 352, 369, 370-379, 860 N.E.2d 307 (Ill. 2006) (claim involving unsolicited faxes under Telephone Consumer Protection Act; "The language of the 'advertising injury' provision is sufficiently broad to encompass the conduct alleged in the complaint"; containing extensive collection of cases); *Valley Forge Ins. Co. v. Swiderski Elecs., Inc.*, 259 Ill. App. 3d, 872, 880-883, 886-887, 834 N.E.2d 562, 569-572, 574-575 (Ill. App. 2005) (intermediate appellate court decision in *Valley Forge*; collecting cases and noting that the majority of federal cases have found claims involving both secrecy and seclusion fall within definition of "privacy"; construing "privacy" to include violations of seclusion); *Hooters of Augusta, Inc. v. Am. Global Ins. Co.*, 272 F. Supp. 2d 1365, 1372-1373 (S.D. Ga. 2003), *aff'd* 157 Fed. Appx. 201(11th Cir. Ga. 2005) (TCPA case involving unsolicited faxes; right to privacy is basically the right to be left alone and a "layman understands his right to be left alone to include being left alone at work by advertisers sending unsolicited faxes. As such, I find that a TCPA violation may constitute an invasion of privacy within the meaning of AGIC's policy"); *Sawyer v. West Bend Mut. Ins. Co.*, 343 Wisc. 2d, 714, 729821 N.W.2d 250, 258 (2012) (right of privacy includes both seclusion and secrecy interests).

disclosure of private information, or secrecy, such as in a data breach, and violations involving intrusion upon seclusion (or the right to be left alone), such as in claims involving unsolicited communications. At the suggestion of carriers, some courts have accepted that the "right of privacy" offense is limited to violations involving secrecy and not seclusion. Other courts have rejected this distinction, in part because "privacy" has at least these two meanings, and is not defined in the CGL policy forms.[24]

Insurers have also tried to avoid coverage by arguing that there was no "publication" of material violating a person's right of privacy. The courts have been divided on whether "publication" requires disclosure to a third party. Some courts have found no such requirement, ruling, in essence, that "publication" can reasonably mean transmittal, such as the transmission of an unwanted message to the claimant, and that no third party disclosure is required.[25] Conversely, carriers have sometimes successfully argued there was no "publication" if the breach did not result in third-party disclosure.[26]

ISO Acts to Eliminate Cyber Coverage under CGL Policies

ISO, which publishes insurance policy forms, has acted steadily to erode potential coverage for cyber-related losses under CGL policies. In the 2001 ISO CGL form, the definition of "property damage"—damage to tangible property—was amended to provide that "electronic data is not tangible property."[27] The 2001 revisions to the ISO CGL form included other restrictions on Coverage B for "personal and advertising injury." Coverage was excluded, with fairly narrow exceptions, for insureds in the businesses of "advertising, broadcasting, publishing or telecasting," "designing or determining content of web sites for others," or "Internet search, access, content or service provider."[28] Coverage was also excluded for personal and advertising injury "arising

---

[24] *See supra*, n.23.

[25] *Valley Forge*, 259 Ill. App. at 885-886, 834 N.E.2d at 573-574 (collecting cases; "Thus, contrary to Insurers' assertion, there is no requirement that the scope of 'publication' be limited to material sent to a third party"; alternatively, finding term ambiguous and to be construed against insurer).

[26] *Recall Total Info. Mgmt. v. Fed. Ins. Co.*, 147 Conn. App. 450, 463-464, 83 A.3d 664, 672-673 (Conn. App. 2014), *aff'd*, 317 Conn. 46 (Conn. 2015) (no "publication" as a matter of law when back-up tapes containing personal information fell out of the back of a truck and were retrieved by an unknown individual, where there was no evidence the information had been accessed or that any person had been harmed). *C.f., Creative Hospitality Ventures, Inc. v. United States Liab. Ins. Co.*, 444 Fed. Appx. 370, 376 (11th Cir. Fla. 2011) (providing a receipt to credit card customer with impermissible personal information is not "publication"; "[t]he receipt is a contemporaneous record of a private transaction between ETL and the customer, and ETL neither broadcasted nor disseminated the receipt or the credit card information to the general public"); *Ticknor v. Rouse's Enters., LLC*, 2 F. Supp. 3d 882, 896 (E.D. La. 2014) (following *Creative Hospitality Ventures*, no "publication" for printing credit card receipt to customer); *see Travelers Prop. Cas. Co. of Am. v. Kan. City Landsmen, L.L.C.*, 592 Fed. Appx. 876, 884-885 (11th Cir. Ga. 2015) (parties agreed term "publication" contemplates dissemination of credit card receipt to at least someone other than the person who provided the card information).

[27] ISO Form CG 00 01 10 01, p. 15 (2001) (definition of "property damage"). The definition of "electronic data" is discussed above.

[28] ISO Form CG 00 01 10 01, p. 6 (2001) (exclusion j).

out of an electronic chatroom or bulletin board the insured hosts, owns, or over which the insured exercises control,"[29] or "arising out of the unauthorized use of another name or product in your e-mail address, domain name or metatag, or any similar tactics to mislead another's potential customers."[30]

In 2007, ISO added an exclusion to Coverage A in its CGL policy form for "damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access or inability to manipulate electronic data."[31] ISO also added exlusions to its standard CGL policy for both Coverage A and Coverage B for claims arising directly or indirectly out of any action or omission that violates or is alleged to violate enumerated statutes, including the Telephone Consumer Protection Act or the CAN-SPAM Act of 2003.[32]

Beginning in 2012, ISO began to publish endorsements designed to drastically limit or completely eliminate any cyber coverage under CGL policies. An endorsement is an amendment to the policy that can either expand, or, as in this case, eliminate coverage.[33] The first form endorsement, issued in 2012, simply eliminated the "privacy" offense from the personal and advertising definition.[34] In 2013, ISO issued a form endorsement that eliminates coverage under Coverage A and Coverage B for damages arising from "any access to or disclosure of any person's or organization's confidential information or personal information, including . . . [specific examples] or any other type of nonpublic information," or the "loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data," with a limited exception for "bodily injury."[35] An alternative form eliminates even the bodily injury exception.[36] It is unclear whether these provisions would exclude coverage for

---

[29] ISO Form CG 00 01 10 01, p. 6 (2001) (exclusion k).

[30] ISO Form CG 00 01 10 01, p. 7 (2001) (exclusion l).

[31] ISO Form CG 00 01 12 07, p. 5 (exclusion p). The definition of "electronic data" was identical to that contained in the 2001 policy form under the definition of "property damage." In the 2013 policy form, this exclusion was amended so as not to apply to liability for damages for "bodily injury," which effectively broadened coverage. ISO Form CG 00 01 04 13, p. 5 (2012).

[32] ISO Form CG 00 01 12 07, pp. 5, 7 (2006) (exclusion q applicable to "bodily injury and property damage" and exclusion p applicable to "personal and advertising injury"). The exclusions also applied to "any statute, ordinance or regulation, other than the TCPA or CAN-SPAM Act of 2003, that prohibits or limits the sending, transmitting, communicating, or distribution of material or information." The ISO policy form for 2013 amended the exclusions to add the Fair Credit Reporting Act ("FCRA"), including the Fair and Accurate Credit Transactions Act ("FACTA") and "any federal state, or local statute, ordinance or regulation . . . that addresses, prohibits, or limits the printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating or distribution of material or information." ISO Form CG 00 01 04 13, pp.5-6 (exclusion q), 7(exclusion p) (2012).

[33] *Ross v. Stephens*, 269 Ga. 266, 269, 496 S.E.2d 705, 708 (1998).

[34] ISO Form CG 24 13 04 13 (2012).

[35] ISO Form CG 21 06 05 14 (2013).

[36] ISO Form CG 21 07 05 14 (2013). Another endorsement applies only to Coverage B and excludes coverage for disclosure of a person's or organization's confidential or personal information. ISO Form CG 08 05 14.

damages for bodily injury or property damaged caused by the manipulation of life safety systems or vehicle controls.

Of course, ISO only makes the forms available and carriers are not obligated to use them. Knowledgeable brokers and agents should try to secure coverage for their insureds without such endorsements, or with the least restrictive endorsement. It appears, however, that the endorsements are gaining traction. An ISO executive commented in a recent interview that, "from some of the feedback we have received to date, it appears that these revisions have been well received by a number of our participating insurers."[37]

Potential Coverage under Other Traditional Insurance Policies

Insureds facing cyber-related claims will also want to consider whether other policies in their insurance portfolio might respond. Although the potential availability of coverage will vary, insureds may find coverage under professional liability policies (also known as "errors and omissions" or "E&O" policies),[38] directors and officers liability policies (also known as "D&O" policies),[39] or crime and fidelity policies.[40]

SPECIFIC COVERAGE FOR CYBER RISKS

Overview

With the insurance industry acting to try to limit coverage under traditional business policies, the good news is that many carriers—including large carriers such as Zurich, ACE, Chubb, and AIG—are now offering various types of cyber coverage. A leading industry consultant reports that, as of mid-2015, rates are rising for larger insureds, particularly retail and healthcare companies, but the market is attractive for small and medium-sized companies with policies available at competitive rates.[41]

---

[37] Interview of Ron Biederman, ISO Assistant Vice President, Commercial Casualty, July 18, 2014, found at http://www.insurancejournal.com/news/east/2014/07/18/332655.htm (last visited July 10, 2015).

[38] *E.g., Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797, 804 (8th Cir. 2010) (finding duty to defend under technology errors and omissions policy); *St. Paul Fire & Marine Ins. Co. v. Compaq Computer Corp.*, 539 F.3d 809, 816 (8th Cir. 2008) (finding duty to defend under technology errors and omissions policy).

[39] *E.g., First Bank of Del., Inc. v. Fid. & Deposit Co. of Md.*, 2013 Del. Super. LEXIS 465, *9 (Del. Super. Ct. Oct. 30, 2013) (finding coverage for losses from data breach under "Electronic Risk Liability" coverage part under Directors and Officers liability insurance policy).

[40] *E.g., Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co.*, 691 F.3d 821, 831-832, (6th Cir. 2012) (finding coverage for $6.8 million in damages caused by a hacking incident under a computer fraud rider to a crime policy).

[41] R. Betterley, *The Betterley Report: Cyber/Privacy Insurance Market Survey 2015*, p. 8 (this Report, which contains detailed summary information regarding policy provisions, is available for purchase at www.irmi.com).

There is no "standard" cyber policy form or program. Many carriers offer package policies that provide a variety of first party and third party coverages which may be quite useful. However, evaluating potential coverage can be difficult due to differences in policy forms and sometimes complicated language.

Businesses considering cyber coverage should first do an internal assessment of their likely risks. Such an assessment would include assessing the types of information maintained by the business, its procedures, and the likely types of claims the business might face. In many instances, the underwriting process may help identify risks.[42] Then, with the assistance of an experienced broker (and perhaps counsel), the business should assess various policy forms and how they would likely respond to the identified risks. No such exercise can be foolproof, but it is a logical place to start.

Examples of Cyber Coverage Forms

As an example, the Zurich Security And Privacy Protection Policy (the "Zurich Specimen Policy") covers damages and defense costs due to a "Security Wrongful Act" or a "Privacy Wrongful Act."[43] A "Security Wrongful Act" is: "any actual or alleged act, error, omission, neglect, or breach of duty by an Insured, someone for whom the Company is legally responsible, or a Service Provider, which causes a breach of the Company's Network Security" that results in:

1. the theft, alteration, destruction, loss or unauthorized release of Electronic Data on the Company's Computer System;
2. the Unauthorized Access to or Unauthorized Use of the Company's Computer System;
3. the denial of an authorized user's access to the Company's Computer System, unless such denial of access is caused by a mechanical or electrical failure outside the control of the Insured;
4. the participation by the Company's Computer System in a Denial of Service Attack directed against a third party's Computer System; or
5. the transmission of Malicious Code from the Company's Computer System to a third party's Computer System.[44]

---

[42] R. Anderson, *Viruses, Trojans, and Spyware, Oh My! The Yellow Brick Road to Coverage in the Land of Internet Oz*, 49 Tort & Ins. L.J. 529 ("The application process itself shines a spotlight on the company's current cybersecurity risk management practices and is likely to reveal potential cybersecurity weaknesses that should be addressed").

[43] Zurich Security And Privacy Protection Policy Specimen, p. 3 (available for download at https://www.zurichna.com/en/industries/technology/secpriv (last visited October 26, 2015) ("Zurich Specimen Policy").

[44] Zurich Specimen Policy, p. 12.

A "Privacy Wrongful Act" "means any actual or alleged act, error, omission, neglect or breach of duty by an Insured, someone for whom the Company is legally responsible, or a Service Provider, that results in a Privacy Event." A "Privacy Event" is:

1. the loss, theft or unauthorized disclosure of:
    a. Personal Information in the care, custody or control of any Insured or Service Provider; or
    b. corporate information in the care, custody or control of any Insured or Service Provider that is specifically identified as confidential or protected under a nondisclosure agreement or similar contract; or
2. a violation of any Privacy Regulation.[45]

The Zurich Specimen Policy also includes a number of potentially significant first party coverages, such as for engaging computer forensics services, providing credit monitoring services, and public relations services. Business interruption coverage is also included for disruption of a company's business operations due to a cyber event. Coverage is also provided for recovering or restoring lost or damaged digital files. The policy also includes coverage for cyber-extortion events, when a company's digital assets are literally held hostage by a malicious intruder. As is the case with any insurance policy, it is necessary to study the defined terms in the policy and the exclusions, policy conditions, sub-limits and other policy provisions in order to assess the true scope of coverage.

Other carriers offer similar policies, although the specific provisions vary, including ACE,[46] AIG,[47] Beazley,[48] and Chubb,[49] along with many others. Companies considering cyber coverage should understand that coverage is often provided in various "coverage parts," and that the combination of coverage parts purchased will affect the total scope of coverage available. Further, particular products may be

---

[45] Zurich Specimen Policy, p. 11. A "Privacy Regulation" means a list of laws "associated with the control and use of personally identifiable financial, medical or other sensitive information," specifically including HIPPA, HITECH, Gramm-Leach Bliley and "any similar state, municipal, federal or foreign identity theft or privacy protection statute, regulation or directive." *Id.*

[46] *E.g.*, ACE DigiTech Digital Technology & Professional Liability Insurance Policy specimen, *available at* http://www.acegroup.com/us-en/assets/ace-digitech-declaration-policy-specimen.pdf (last visited on October 26, 2015).

[47] AIG CyberedgeSecurity and Privacy Liability Insurance specimen, *available at* http://www.aig.com/-Chartis/internet/US/en/SECURITY%20AND%20PRIVACY%20COVERAGE%20SECTION%20101024%20(12-13)%20SRP%20Coverage%20Parts_tcm3171-661710.pdf (last visited on October 26, 2015).

[48] Beazley AFB Media Tech Professional And Technology Based Services, Technology Products, Information Security & Privacy, And Multimedia And Advertising Liability Insurance Policy, *available at* https://www.beazley.com/Documents/Private%20Enterprise/Wordings/Media_Tech_E0_2014_Policy_Form.pdf (last visited on October 26, 2015).

[49] Chubb Forefront Portfolio 3.0CyberSecurity Coverage Part, *available at* http://www.chubb.com/businesses/csi/chubb13765.pdf (last visited October 26, 2015).

marketed only to companies of a particular size, and some carriers may not write coverage for all industries.

Potential Pitfalls

There are many potential pitfalls in purchasing cyber coverage, and a detailed treatment is beyond the scope of this article. A few common pitfalls, however, should be emphasized:

- *Claims made coverage/retroactive date.* Cyber coverage is written on a claims made basis.
  - Unlike occurrence policies, which cover liabilities arising from acts or omissions happening during the policy period regardless of when a claim is made or a lawsuit is filed, clams made policies cover only claims made during the policy period or any applicable extended reporting period.
  - Most claims made policies also have a "retroactive date," or "retro date," and cover only claims that arise from *acts or omissions* that occur *after* the retroactive date. Accordingly, even if a claim is made during the policy period, it will not be covered if it arose from acts or omissions occurring before the retro date.
  - Because the retro date cuts off a carrier's liability for claims based on acts going back in time, and the "claims made" requirement eliminates coverage for claims made after the policy period (or extended reporting period), placing claims made coverage to avoid unexpected gaps can be tricky. These requirements can also create gaps in the event that an insured switches carriers. It is important to involve an experienced broker or other professional to address these issues.
- *Coverage for Contractors and Cloud-Based Resources.* Many companies outsource all or part of their IT to third-party contractors. Some companies completely outsource their operations to a cloud provider, and store their own information, and their customers' information, in the "cloud." In these situations, it is important for the policy to cover breaches and liabilities caused by independent contractors, or that occur on the "computer" or "computer systems" owned and maintained by the cloud provider for use in the insured's business.
- *Exclusions.* All policies have exclusions and that should be carefully reviewed before placing coverage. Several important exclusions that may find their way into cyber policies and which should be avoided include:
  - *Failure to Follow "Minimum Practices."* Some, but not all, cyber policies contain exclusions for failure to follow "minimum practices" listed in the insured's application, or for failure to apply software patches or other security measures. One insurer recently filed suit against an insured seeking to recoup payments the insurer had advanced to settle a breach.[50]

[50] *Columbia Casualty Company v. Cottage Health System*, Civil Action File No. 2:15-cv-03432 (C.D. Ca. May 17, 2015).

This is one of the first cases to test such an exclusion and is being closely watched by coverage lawyers.

- *Criminal or Fraudulent Acts.* Most policies have an exclusion for claims resulting from criminal or fraudulent acts. However, many policies require an actual conviction or guilty plea. Policies may also contain "separation of insureds" provisions or other language such that the bad conduct of one insured is not imputed to the company or other insureds. Businesses should seek the most generous provisions.
- *Acts of War or Terrorism by Governmental or Non-Governmental Entities.* Some cyber policies have adopted exclusions from general liability policies seeking to avoid coverage for claims or losses resulting from acts or war or terrorism. Given that certain well-known attacks were allegedly perpetrated by government actors,[51] businesses should seek cyber coverage without such exclusions.

Unknowns

Although cyber coverage appears to be a wise investment for many businesses, there are important unknowns that may affect its practical value. First, cyber coverage is so new that coverage lawyers and brokers have little experience in assessing how insurance company claims departments will respond in handling claims, which, as a practical matter can be just as important as what the policy says.[52] Second, there has been a dearth of court cases assessing coverage under the newer policies, and it is unclear how the courts will react to claims for cyber coverage.

Further, the cyber threat continues to evolve. Malicious actors are always looking for new ways to exploit cyber vulnerabilities. Although some current cyber insurance offerings seem reasonably well-suited to known risks, it is not clear how policy wording will respond to new and currently unknown risks and attacks.

CONCLUSION

Businesses and insurers remain in the very early innings of the battle against cyber threats. Just as insurers are trying to eliminate coverage for cyber risks under most

[51] *FBI Says North Korea Behind Sony Hack*, *Wall Street Journal*, December 19, 2014 (*available at* http://www.wsj.com/articles/fbi-says-north-korea-behind-sony-hack-1419008924?alg=y) (last visited October 26, 2015).

[52] The author was involved in a claim made by an insured under one of the newer policy forms that specifically covered liability for alleged trade secret violations. Nevertheless, the carrier took the position that trade secret violations were not covered, which required the insured to institute litigation to obtain a satisfactory outcome.

traditional business policies, they are offering a wide variety of options for specific cyber coverage. It is important for businesses to assess their risks carefully, and to try to ensure their coverage options are tailored to meet those risks. With a wide variety of policy forms, but very little current experience regarding how claims will be handled under the new policies, the current environment is both encouraging and challenging.