Chapter 16

Insurance Coverage for Data Breaches and Unauthorized Privacy Disclosures

Steven R. Gilford*

Proskauer Rose LLP

* The author would like to thank Proskauer associates Jacki Anderson, Michael Derksen and Bradley Lorden for their invaluable contributions in writing and updating this chapter and Proskauer summer associates Anum Chaudhry and Zachary Zermay for their work on researching updates to its 2015 supplement.

§ 16:1 Overview

The unauthorized disclosure of personal and other confidential information has become a well-known and ever-increasing risk for holders of third-party information and business data. Notification letters from companies that have suffered data breaches have become common occurrences, and high-profile breaches of millions of records at major companies have become the subject of headlines and board of directors meetings around the world.[1]

In addition to asserted claims of data privacy breaches, risks from technology exposures include business interruption, inability to perform obligations to others, and loss or distortion of company and client data. As businesses continue to evolve and change in an environment driven by technology, so too does the handling of sensitive information and data. Due to the ubiquity and increasing quantity of digital data, holders of information are exposed to a multitude of risks that

1. *See, e.g.*, Maria Korolov, *Cybersecurity on the Agenda for 80 Percent of Corporate Boards*, CSO (May 28, 2015), www.csoonline.com/article/2927395/data-protection/cybersecurity-on-the-agenda-for-80-percent-of-corporate-boards.html.

data can be lost or stolen.[2] The costs associated with a data breach or unauthorized disclosure of confidential information can be substantial,[3] and they are likely to continue to increase as governmental regulators become increasingly vigilant and sophisticated in the regulation of cyber privacy issues and concerns.[4] At the same time, corporate directors and officers are facing increased exposure to liability in relation to data breaches, as plaintiffs' attorneys have endeavored to hold them responsible for allegedly inadequate attention to data security.[5]

As the risks associated with data and privacy breaches continue to grow and evolve, companies and individuals have turned, in varying degrees, to their insurers for protection. According to a recent report, procurement of cyber insurance policies by clients of one leading broker increased by 27% from 2014 to 2015, with companies in the manufacturing, communications, and technology industries having the highest growth in demand.[6] Historically, claims for insurance for these types of risks have been asserted under traditional coverages, including commercial general liability (CGL) policies, directors and officers (D&O) liability insurance, errors and omissions (E&O) policies, and commercial crime and first-party property and business

---

2. Data loss or security breaches can occur in a number of ways, including network hacking, lost or stolen laptops, spyware, phishing, insecure media disposal, hacked card swiping devices, security vulnerabilities on mobile devices, misdirected mail and faxes, insecure wireless networks, peer-to-peer software, breaches in physical security, problematic software updates or upgrades, human error, rogue or disgruntled employees, and lost or stolen media. Even companies that focus on storing passwords have been hacked. *See, e.g.*, Jose Pagliery, *Irony Alert: Password-storing Company Is Hacked*, CNN, June 16, 2015, http://money.cnn.com/2015/06/15/technology/lastpass-password-hack/index.html.

3. In 2016, the costs of a compromised record reportedly averaged $221 per record, and the average cost per data breach event was over $7 million per event, increasing from $6.5 million per event in 2015 (with some events costing tens of millions of dollars). PONEMON INSTITUTE LLC, 2016 COST OF DATA BREACH STUDY: UNITED STATES (June 2016), www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094USEN.

   Costs associated with a typical data breach can include, but are not limited to, internal investigation costs, forensic experts, consumer notification, credit monitoring, crisis management, call center services, attorney fees, payment card industry fines, increased processing fees, damages, awards and settlements, agency and attorney general actions, reputational costs, and technology upgrades. *Id.*

4. *See* section 16:3.3, *infra*.

5. *See* section 16:2.3[A], *infra*.

6. *Benchmarking Trends: Operational Risks Drive Cyber Insurance Purchases*, Marsh & McClennan (Mar. 23, 2016), www.marsh.com/us/insights/research/cyber-benchmarking-trends-2016.html.

interruption policies. Insurers, however, have frequently taken the position that these traditional coverages do not cover claims for data and privacy breaches.

An insurance coverage case filed by Arch Insurance Company against Michaels Stores is illustrative.[7] Michaels Stores faced a series of lawsuits alleging that it had failed to safeguard customers against a security breach related to its credit and debit PIN pad terminals. Customers alleged that Michaels' failure to secure PIN pad terminals allowed criminals to access customer financial information and to make unauthorized withdrawals and purchases. Michaels sought coverage under its traditional form CGL policy. Arch, the insurer, sued Michaels in federal court in Chicago, claiming that its policy did not cover the losses and seeking a declaration that it had no duty to defend or indemnify Michaels against the underlying claims. In the coverage lawsuit, Arch claimed that the alleged property damage in the underlying complaint was not covered because "electronic data" was excluded from the definition of tangible property. It also contended that the policy excluded damages arising out of the "loss or, loss of use, or damage to, corruption of, inability to access, or inability to manipulate electronic data."

Whether you agree with the position taken by the insurer or not, these cases are not uncommon. In recent years, similar cases have been brought involving Zurich American Insurance,[8] Colorado Casualty,[9] Landmark American Insurance,[10] Federal Insurance,[11]

---

7. Complaint, Arch Ins. Co. v. Michaels Stores Inc., No. 12-0786 (N.D. Ill. Feb. 3, 2012) (case settled following summary judgment briefing without disposition).
8. Complaint, Zurich Am. Ins. Co. v. Sony Corp. of Am., No. 651982/2011 (N.Y. Sup. Ct. July 20, 2011) (insurer claimed it was not obligated to defend or indemnify against a class action suit for hackers' theft of identification and financial information; Zurich claimed theft of the information did not fall within policy coverage areas of "bodily injury," "property damage," or "personal and advertising injury"). For further discussion, see *infra* note 69 and accompanying text.
9. Colo. Cas. Ins. Co. v. Perpetual Storage, Inc., 2011 U.S. Dist. LEXIS 34049 (D. Utah Mar. 30, 2011) (insurer claimed that Perpetual Storage's insurance policy did not cover its liability for theft of a client university's computer backup tapes containing sensitive medical records).
10. Landmark Am. Ins. Co. v. Gulf Coast Analytical Labs. Inc., 2012 U.S. Dist. LEXIS 45184 (M.D. La. Mar. 26, 2012) (insurer sought declaratory judgment that its policy did not cover a third-party claim related to data lost when Gulf Coast accidentally corrupted a client's hard drives).
11. Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 115. A.3d 458 (Conn. 2015) (insurer claimed that Recall's policy did not cover liability for loss of electronic data on computer tapes containing personal information of IBM employees). For further discussion, see section 16:2.2, *infra*.

Travelers,[12] Columbia Casualty,[13] and National Fire of Hartford,[14] to name just a few. A similar line of cases exists in the first-party property context where carriers have taken the position that there is no coverage for costs incurred to respond to a security breach, usually on the theory that the loss of electronic data is not "physical" and therefore is not covered under a policy that insures only "physical loss" or "physical damage" to covered property.[15] More recently, CGL and traditional property insurance policies have tended to include specific exclusions aimed at eliminating coverage for cyber risks in their entirety or at least in part.[16]

---

12. Complaint, Travelers Indem. Co. of Conn. v. P.F. Chang's China Bistro, Inc., 14-cv-01458 (D. Conn. Oct. 2, 2014) (seeking declaration that insurer has no duty to defend or indemnify insured for underlying lawsuits stemming from a data breach that alleged the insured failed to properly safeguard its customers' information).

13. Complaint, Columbia Cas. Co. v. Cottage Health Sys., No. 15-cv-03432 (C.D. Cal. May 7, 2015) (seeking a declaration that there was no coverage under the insured's "NetProtect 360" cyber policy for an underlying class action lawsuit stemming from a data breach of over 30,000 confidential medical records).

14. Nat'l Fire Ins. Co. of Hartford v. Med. Informatics Eng'g, Inc., No. 1:16-cv-00152 (N.D. Ind. May 13, 2016) (seeking declaration that insurers do not have to defend or indemnify their insured for multidistrict litigation over a data breach affecting 3.9 million patients, on grounds that claim falls outside insured's general liability policies and is barred by several exclusions).

15. *E.g.*, Ward Gen. Ins. Servs., Inc. v. Emp'rs Fire Ins. Co., 7 Cal. Rptr. 3d 844 (Dist. Ct. App. 2003) (data loss due to computer crash and human error did not constitute a loss of tangible property under first-party policy); Greco & Traficante v. Fid. & Guar. Ins. Co., 2009 Cal. App. LEXIS Unpub. 636, at *12–13 (Ct. App. Jan. 26, 2009) (data lost due to power outage that did not damage physical media, such as disks, not covered by first-party policy); *cf.* St. Paul Fire & Marine v. Nat'l Comput. Sys., Inc., 490 N.W.2d 626, 631 (Minn. Ct. App. 1992) (misuse of trade secret information stored in binders did not constitute damage to tangible property because "the information itself was not tangible"); *see* section 16:2.1[A], *infra*.

16. *See, e.g.*, ISO Endorsement CG 21 07 05 14 (2013) (excluding "(1) [a]ny access to or disclosure of any person's or organization's confidential or personal information, including . . . financial information, credit card information, health information or any other type of nonpublic information; or (2) the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data"); Complaint, Arch Ins. Co. v. Michaels Stores Inc., No. 12-0786 (N.D. Ill. Feb. 3, 2012) (asserting that policy at issue excludes "electronic data" from the definition of tangible property); Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co., 2012 Conn. Super. LEXIS 227 (Super. Ct. Jan. 17, 2012) (definition of property damage provided that "tangible property does not include any software, data or other information that is in electronic form."), *aff'd*, 115 A.3d 458 (Conn. 2015); *see* notes 29, 32, 47, and 73, *infra*. *See generally* 2 STUART

Given these lines of cases, the substantial costs associated with litigating a major coverage case, and the tactical complexities of having to simultaneously deal with claims from a cyber loss and prosecute or defend an insurance dispute, businesses have sought more clearly applicable coverages. Insurers have responded by developing insurance products specifically designed to respond to cyber issues with a panoply of names such as network risk policies, cyber insurance, and network security liability, and privacy liability and data loss policies.[17] Insurers have also developed endorsements to traditional policies that may extend various coverages to cyber risks,[18] though those endorsements are often narrowly drawn.[19] New policy offerings may present opportunities to close gaps in an existing coverage program; however, these new insurance products should be carefully evaluated to compare the coverage offered to a particular company's cyber risk profile, including its exposure to data and privacy breaches and to insurance already available from traditional coverages.

The next section of this chapter discusses some of the issues that have arisen from the application of traditional coverages to cyber losses

---

A. PANENSKY ET AL., DATA SEC. & PRIVACY LAW § 14:23 (2015) (stating that a recent version of the ISO Commercial General Liability Coverage form specifically excludes electronic data as tangible property in its definition of property damage); Ins. Servs. Office, Inc., Commercial General Liability Coverage Form CG 00 01 10 01, § V (17)(b) (2008), LEXIS, ISO Policy Forms ("For the purposes of this insurance, electronic data is not tangible property. As used in this definition, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media . . . .").

17. *See, e.g.*, *CyberFirst*, TRAVELERS, www.travelers.com/business-insurance/cyber-security/technology/cyber-first.shtm (last visited Aug. 16, 2016); *see also* CHUBB CyberSecurity Form 14-02-14874, § I.J. (2009); Philadelphia Insurance Co. Cyber Security Liability Coverage Form PI-CYB-001, § I.C. (2010).

18. *See, e.g.*, Complaint, Clarus Mktg. Grp., LLC v. Phil. Indem. Ins. Co., No. 11-2931 (S.D. Cal. 2011) (the "Network Security and Privacy Liability Coverage Endorsement" covered damages against "any actual or alleged breach of duty, neglect, act, error or omission that result[s] in a Privacy Breach"; the parties ultimately settled and filed a joint motion to dismiss).

19. *See, e.g.*, Universal Am. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA, 38 Misc. 3d 859 (N.Y. Sup. Ct.) (coverage denied because "Computer Systems Fraud" rider to the insured's Financial Institution Bond was not intended to cover "fraudulent claims which were entered into the system by authorized users"), *aff'd*, 110 A.D.3d 434 (N.Y. App. Div. 1st Dep't 2013); Tornado Techs., Inc. v. Quality Control Inspection, Inc. 977 N.E.2d 122 (Ohio Ct. App. 2012) (coverage denied because "Computer Coverage Form" did not apply to the location where back-up servers were located).

and privacy breaches. While there is still only limited case law analyzing new cyber policies, the chapter then discusses some of the important issues to consider in evaluating these more recent forms.

§ 16:2 Applicability of Historic Coverages

Though there are a variety of potentially applicable coverages, traditional insurance for privacy and security breaches is most commonly sought under an insured's CGL or property policies. Both types of policies cover losses relating to damage to property. CGL policies also provide coverage for certain specified types of "advertising injury" and "personal injury," which sometimes, particularly under older forms, may include invasion of privacy.

§ 16:2.1 First- and Third-Party Coverages for Property Loss

Insurance practitioners typically distinguish between two types of coverage—first-party coverage, which generally insures a loss to the insured's own property, and third-party coverage, which generally provides insurance for liability claims asserted against the insured by third parties for damage to the claimant's property.[20]

In the absence of dispositive exclusions for cyber risks, the availability of coverage for privacy breaches or other cyber risks under either a first-party property policy or the property coverage provision of a third-party CGL policy usually turns on the issue of whether the loss of computer data or information constitutes "physical damage" to "tangible property" under the governing policy language. Although first-party and third-party coverages apply to different types of losses, the same definitional issues are often raised by insurers and analyzed by courts assessing the availability of each kind of coverage. In each case, "property damage" is typically defined in the policy or by case law 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."[21]

---

20. *See, e.g.*, Port Auth. v. Affiliated FM Ins. Co., 245 F. Supp. 2d 563, 577 (D.N.J. 2001) (explaining that third-party "liability insurance, which indemnifies one from liability to third persons, is distinct from first-party coverage, which protects against losses sustained by the insured itself") (citation omitted), *aff'd*, 311 F.3d 226 (3d Cir. 2002). *See generally* ALLAN D. WINDT, INSURANCE CLAIMS AND DISPUTES §§ 6:5 & 6:6 (6th ed. 2013).

21. *See, e.g.*, Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797, 801–02 (8th Cir. 2010) (liability insurance policy defined "property damage" 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"); Big

Courts are divided as to whether property losses relating to computer infrastructure and data resources constitute "physical injury" to "tangible property" for purposes of an insurance claim. While cases have held repeatedly that physical damage to computer hardware is covered under first- and third-party insurance policies,[22] courts have sometimes struggled with the issue of whether damage to data alone qualifies as physical injury to tangible property.[23]

[A] First-Party Property Policies

Cases are divided over whether lost data is covered under first-party property policies. While some courts have taken the position that software and data are not tangible property,[24] others have applied a

---

Constr., Inc. v. Gemini Ins. Co., 2012 WL 1858723, at *8 (W.D. Wash. May 22, 2012) (construction company sued insurer for coverage in underlying suit where policy defined "property damage" as "Physical injury to tangible property, including all resulting loss of use of that property" and "Loss of use of tangible property that is not physically injured"); Auto-Owners Ins. Co. v. Pozzi Window Co., 984 So. 2d 1241, 1244 (Fla. 2008) (same); Mangerchine v. Reaves, 63 So. 3d 1049, 1055 n.5 (La. Ct. App. 2011) (in first-party claim against insurer, policy defined "property damage" as "physical injury to, destruction of, or loss of use of tangible property"). *See generally* ALLAN D. WINDT, INSURANCE CLAIMS AND DISPUTES § 11:1 (6th ed. 2013).

22. *E.g.*, Lambrecht & Assocs., Inc. v. State Farm Lloyds, 119 S.W.3d 16, 23–25 (Tex. App. 2003) (holding that first-party policy covered data losses due to damage to computer server: "the server falls within the definition of 'electronic media and records' because it contains a hard drive or 'disc' which could no longer be used for 'electronic data processing, recording, or storage'"); Nationwide Ins. Co. v. Hentz, 2012 U.S. Dist. LEXIS 29181 (S.D. Ill. Mar. 6, 2012), *aff'd*, Nationwide Ins. Co. v. Cent. Laborers' Pension Fund, 704 F.3d 522 (7th Cir. 2013) (finding "property damage" under homeowner's insurance policy since the insured's losses resulted from the theft of a CD-ROM, which constituted "tangible property"; however, an exclusion still applied to bar coverage); Cincinnati Ins. Co. v. Prof'l Data Servs., Inc., 2003 WL 22102138 (D. Kan. July 18, 2003) (for purposes of third-party coverage; damage to computer hardware constitutes "property damage" and would trigger coverage, but damage to software alone does not).

23. *See* section 16:2.1[A]–[B], *infra*.

24. *See, e.g.*, Liberty Corp. Capital Ltd. v. Sec. Safe Outlet, Inc., 937 F. Supp. 2d 891, 901 (E.D. Ky. 2013) (email addresses stolen from electronic databases did not constitute "tangible property" and were excluded by policy's exclusion of "electronic data"); Metro Brokers, Inc. v. Transp. Ins. Co., 603 F. App'x 833 (11th Cir. 2015) (holding that the insured's first-party property policy's coverage of "forgery" applied only to so-called traditional negotiable instruments and, therefore, there was no coverage for the fraudulent electronic transfer of money from the insured's client's escrow accounts); Greco & Traficante v. Fid. & Guar. Ins. Co., 2009 Cal. App. Unpub. LEXIS 636, at *12–13 (Ct. App. Jan. 26, 2009) (data lost due to power outage that did not damage physical media such as disks or

broader definition of "physical damage" and held that data itself constitutes physical property.[25] In addition, various cases have held that the inability to use a computer due to damaged data may constitute a "loss of use" and thus covered property damage under a first-party policy,[26] at least in the absence of an applicable exclusion of wear and tear or a latent defect.[27]

While decisions have found coverage for lost or damaged data as property damage under traditional first-party property policies,[28] many insurers have responded by taking steps to exclude electronic

---

computers was not covered by a first-party property policy); Ward Gen. Servs., Inc. v. Emp'rs Fire Ins. Co., 7 Cal. Rptr. 3d 844 (Ct. App. 2003) (data loss due to a computer crash and human error did not constitute a loss of tangible property under a first-party policy).

25. *See, e.g.*, NMS Servs., Inc. v. Hartford, 62 F. App'x 511, 515 (4th Cir. 2003) (concurring opinion by Judge Widener stated that data erased by a hacker was a "direct physical loss"); Landmark Am. Ins. Co. v. Gulf Coast Analytical Labs., Inc., 2012 U.S. Dist. LEXIS 45184 (M.D. La. Mar. 26, 2012) (electronic data, while not tangible, is physical, and therefore susceptible to "direct, physical 'loss or damage'"); Se. Mental Health Ctr., Inc. v. Pac. Ins. Co., 439 F. Supp. 2d 831 (W.D. Tenn. 2006) (first-party property policy covered loss of use of a computer as "property damage" after loss of stored programming information and configurations); Am. Guar. & Liab. Ins. Co. v. Ingram Micro, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. Apr. 18, 2000) (reasoning, based on an analysis of state and federal criminal statutes, that the loss of data constitutes physical damage under first-party business interruption policy); S. Cent. Bell Tel. Co. v. Barthelemy, 643 So. 2d 1240, 1244 (La. 1994) (electronic software data is physical); Comput. Corner, Inc. v. Fireman's Fund Ins. Co., 46 P.3d 1264, 1266 (N.M. Ct. App. 2002) (computer data is physical, and its loss is covered under third-party policy).

26. *See, e.g.*, Se. Mental Health Ctr., Inc. v. Pac. Ins. Co., 439 F. Supp. 2d 831 (W.D. Tenn. 2006) ("property damage" includes not only "physical destruction or harm of computer circuitry, but also loss of access, loss of use, and loss of functionality," so a first-party property policy covered loss of use of a computer after loss of stored programming information and configurations); Lambrecht & Assocs., Inc. v. State Farm Lloyds, 119 S.W.3d 16, 23–24 (Tex. App. 2003) (loss of use of computers, as well as loss of data, constituted a physical loss and fell within the scope of policy coverage); Metalmasters of Minn., Inc. v. Liberty Mut. Ins. Co., 461 N.W.2d 496, 502 (Minn. Ct. App. 1990) (data loss was covered by first-party property policy because computer tapes themselves were physically damaged in flood).

27. *See, e.g.*, GF&C Holding Co. v. Hartford Cas. Ins. Co., No. 11-cv-00236, 2013 U.S. Dist. LEXIS 38669, at *9–10 (D. Idaho Mar. 15, 2013) (finding property damage where insured's hard drives failed, but holding coverage unavailable where exclusion provided that insurer "will not pay for physical loss or physical damage caused by or resulting from . . . wear and tear . . . [or] latent defect").

28. *See supra* notes 25–26.

data from the definition of tangible property.[29] Indeed, the Insurance Services Office amended the definition of property damage in 2001 to specifically omit coverage for "electronic data"[30] and, in 2004, added an exclusion for "[d]amages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."[31] Therefore, first-party property policies currently available in the market often do not typically provide coverage for data breaches unless computer hardware has been physically damaged.[32]

[B] Third-Party CGL Policies: Coverage for Property Damage Claims

Courts have similarly been mixed in deciding whether data losses constitute covered property damage in the context of third-party CGL policies. In some cases, the courts have found that liability based on loss of data does not trigger coverage.[33] For example, in *America*

---

29. *See, e.g.*, RVST Holdings, LLC v Main St. Am. Assurance Co., 136 A.D.3d 1196 (N.Y. App. Div. 3d Dep't 2016) (denying coverage for third-party claim arising out of data breach, reasoning that the policy provided that "electronic data is not tangible property" and excluded "[d]amages arising out of the loss of . . . electronic data"); *Liberty Corp. Capital*, 937 F. Supp. 2d at 901 (no coverage for misappropriation of email addresses from electronic databases based on finding that customer email list "property" does not fall within definition of "tangible property" and also excluded under electronic data exclusion); Recall Total Info. Mgmt. v. Fed. Ins. Co., 2012 Conn. Super. LEXIS 227 (Super. Ct. Jan. 17, 2012), *aff'd*, 83 A.3d 664 (Conn. App. Ct.), *aff'd*, 115 A.3d 458 (Conn. 2015) (because electronic data was specifically excluded, coverage did not exist under CGL and umbrella policies for notification and other costs incurred when unencrypted data tapes containing personal information fell from the back of a truck and were stolen; court found that damage arose from the data, not the actual tapes); Ins. Servs. Office, Inc., Commercial Liability Umbrella Form 00 01 12 04 § V(18)(b) (2004), LEXIS, ISO Policy Forms ("For the purposes of this insurance, electronic data is not tangible property."). *See generally* 3 MARTHA A. KERSEY, NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 18.02[4][a] (2015) (standard CGL policy form now defines electronic data and specifically excludes it from the definition of property damage).

30. *See, e.g.*, Jeff Woodward, *The 2001 ISO CGL Revision*, INT'L RISK MGMT. INST., INC. (Jan. 2002), www.irmi.com/articles/expert-commentary/the-2001-iso-cgl-revision.

31. *See, e.g.*, Jeff Woodward, *The 2004 ISO CGL Policy*, INT'L RISK MGMT. INST., INC. (Apr. 2004), www.irmi.com/articles/expert-commentary/the-2004-iso-cgl-policy.

32. *See, e.g.*, Greco & Traficante v. Fid. & Guar. Ins. Co., 2009 Cal. App. Unpub. LEXIS 636, at *12–13 (Ct. App. Jan. 26, 2009) (because computer and disks were not damaged, data loss was not covered by a first-party property policy).

33. *See, e.g.*, Am. Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89 (4th Cir. 2003) (discussed in following text); State Auto Prop. & Cas. Ins. Co. v. Midwest Computs. & More, 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001) (reasoning that computer data is not tangible property).

Online, Inc. v. St. Paul Mercury Insurance Co.,[34] the Fourth Circuit concluded that damage to and loss of use of customers' data and software were not covered under a CGL policy because there was no damage to "tangible property" under the definition of "property damage."[35] The court reasoned that computer data was "an abstract idea in the minds of the programmer and the user," so loss or damage to software or data was "not damage to the hardware, but to the idea."[36]

Other courts have applied a broader definition of "physical damage" and held that data constitutes physical property.[37] For example, in *Computer Corner, Inc. v. Fireman's Fund Insurance Co.*, the court reasoned that because computer data "was physical, had an actual physical location, occupied space and was capable of being physically damaged and destroyed," that lost data was covered under a CGL policy.[38] In addition, courts have held that an alleged "loss of use" may constitute covered property damage under a CGL policy, where there is appropriate policy wording.[39]

A leading authority in this area is the decision of the U.S. Court of Appeals for the Eighth Circuit in *Eyeblaster, Inc. v. Federal Insurance Co.*[40] In that case, Eyeblaster, an Internet advertising company, sought coverage under two policies, a general liability policy and an information and network technology errors and omissions liability policy, for claims alleging that its products had caused damage to a user's computer.[41] After stating that the plain meaning of "tangible property" includes computers,[42] the Eighth Circuit ruled that the claims against Eyeblaster fell within the CGL policy because the underlying suit repeatedly alleged a "loss of use" of a computer.[43] The court found coverage under these circumstances even though the CGL policy excluded

---

34. Am. Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89 (4th Cir. 2003).
35. *Id.* at 96.
36. *Id.* at 95–96.
37. Comput. Corner, Inc. v. Fireman's Fund Ins. Co., 46 P.3d 1264 (N.M. Ct. App. 2002) (discussed *infra*); *see also* NMS Servs., Inc. v. Hartford, 62 F. App'x 511, 515 (4th Cir. 2003) (Widener, J. concurring) (stating that data erased by a hacker was a "direct physical loss"); Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797 (8th Cir. 2010) (discussed in following paragraph).
38. *Computer Corner*, 46 P.3d at 1266.
39. *See, e.g.*, State Auto Prop. & Cas. Ins. Co. v. Midwest Comput. & More, 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001) (computer data was not tangible property, but a computer is tangible property so loss of use of that property constitutes property damage where the policy includes coverage for "loss of use of tangible property").
40. Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797 (8th Cir. 2010).
41. *Id.* at 799.
42. *Id.* at 802.
43. *Id.*

electronic data from the definition of "tangible property."[44] According to the court, the alleged "loss of use" of the physical computer hardware implicated coverage under the policy.[45] Under this approach, though the loss of data itself may not be covered because it fails to qualify as damage to tangible property, the loss of use of computer hardware due to a loss of data may allow coverage.

Although some decisions find that lost or corrupted data or loss of use constitutes property damage,[46] evolving policy definitions and exclusions in CGL policies now often state specifically that electronic data is not tangible property covered under property damage provisions or exclude damages arising out of the loss of use of electronic data.[47] As a result, policyholders seeking coverage for a data loss under the property damage provisions of a traditional CGL policy may find it increasingly difficult to obtain coverage. While insureds confronted with a loss should evaluate the availability of coverage under property damage provisions of CGL policies, another successful avenue for coverage of data breach and privacy claims—at least in the liability context—is often found in the coverage for personal and advertising injury.

§ 16:2.2 CGL Coverage for Personal and Advertising Injury Claims

CGL policies typically provide liability coverage for damages arising from claims against the insured that involve bodily injury, property damage, advertising injury, and personal injury. While insurers continue to add exclusions in an effort to restrict insurance for cyber claims,[48] in addition to property damage coverage discussed

---

44. *Id.*
45. *Id.*
46. *E.g.*, Se. Mental Health Ctr., Inc. v. Pac. Ins. Co., 439 F. Supp. 2d 831, 838 (W.D. Tenn. 2006); Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc., 2000 U.S. Dist. LEXIS 7299, at *10 (D. Ariz. Apr. 18, 2000); *Eyeblaster*, 613 F.3d at 802.
47. *See, e.g.*, *Eyeblaster*, 613 F.3d at 802 (definition of "tangible property" excludes "any software, data or other information that is in electronic form"); Ins. Servs. Office, Inc., Commercial Liability Umbrella Form CU 00 01 12 04 § V(18)(b) (2004), *available at* LEXIS, ISO Policy Forms ("For the purposes of this insurance, electronic data is not tangible property."); Ins. Servs. Office, Inc., Commercial Liability Umbrella Coverage Form CU 00 01 12 04 § A.2.t (2004), *available at* LEXIS, ISO Policy Forms (excluding "damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access or inability to manipulate electronic data").
48. The April 2013 revisions to the ISO CGL form introduced a new endorsement entitled "Amendment of Personal and Advertising Injury Definition." This endorsement explicitly excludes the right of privacy provision from paragraph 14.e. of the Personal and Advertising Injury definitions section

above,[49] coverage for data breaches and privacy-related claims may exist under CGL policy provisions insuring "personal injury" and "advertising injury," particularly where they include coverage for liability arising from "oral or written publication, in any manner, of material that violates a person's right of privacy."[50]

Personal and advertising injury provisions often limit coverage to specifically enumerated offenses like malicious prosecution or copyright infringement.[51] For coverage of data breaches, the most important of these enumerated offenses is usually "oral or written publication, in any manner, of material that violates a person's right of privacy."[52] Some policies and courts limit coverage for violation of a right to privacy to injuries caused by an insured's "advertising"

("[o]ral or written publication, in any manner, of material that violates a person's right of privacy"). Ins. Servs. Office, Inc., Commercial Liability Form CG 24 13 04 13 (2013), *available at* LEXIS, ISO Policy Forms; *see also* section 16:2.1[B], *supra*.

49. *See* section 16:2.1, *supra*.

50. Two illustrative provisions are as follows:

> "Personal injury" is defined as an injury, other than "bodily injury,'" arising out of certain enumerated offenses including: 1) false arrest, detention or imprisonment, 2) malicious prosecution, 3) wrongful eviction from, wrongful entry into, or invasion of the right of private occupancy of a room, dwelling or premises that a person occupies by or on behalf of its owner, and lord or lessor, 4) oral or written publication of material that slanders or libels a person or organization or disparages a person's or organization's goods, products, or services, or 5) *oral or written publication of material that violates a person's right of privacy*."
>
> 9A STEVEN PLITT ET AL., COUCH ON INSURANCE § 129:7 (3d ed. 2014) (emphasis added).
>
> "Advertising injury" is defined as injury arising out of certain enumerated offenses, including: 1) oral or written publication of material that slanders or libels a person or organization or disparages a person's or organization's goods, products, or services; 2) *oral or written publication of material that violates a person's right of privacy*; 3) misappropriation of advertising ideas or style of doing business; or 4) infringement of copyright, title, or slogan.
>
> *Id.* § 129:8 (emphasis added); *see, e.g.*, Zurich Am. Ins. Co. v. Fieldstone Mortg. Co., 2007 U.S. Dist. LEXIS 81570, at *3–4 (D. Md. Oct. 26, 2007). *But see* note 48, *supra*.

51. 9A STEVEN PLITT ET AL., COUCH ON INSURANCE § 129:8 (3d ed. 2014); *see* note 50, *supra*.

52. *See, e.g.*, Ins. Servs. Office, Inc., Commercial General Liability Form CG 00 01 10 01, § V(14)(e) (2008), *available at* LEXIS, ISO Policy Forms; notes 48–49, *supra*; *see also* Hartford Cas. Ins. Co. v. Corcino & Assocs., 2013 U.S. Dist. LEXIS 152836 (C.D. Cal. Oct. 7, 2013) (holding that a hospital data breach was covered under the CGL policy provision that includes

activity,[53] but many include this coverage for any publication.[54] When seeking insurance under the personal or advertising injury clauses of a traditional CGL policy, insurers will often contest coverage based on arguments that the policyholder's actions did not amount to a publication of information or that a third party's right to privacy was not implicated.[55]

"electronic publication of material that violates a person's right of privacy"); *but see* ISO Form CG 24 13 04 13 (2012) (specifically excluding violation of right to privacy as an enumerated offense), quoted in note 46, *supra*.

53. 3 ALLAN D. WINDT, INSURANCE CLAIMS AND DISPUTES § 11:29 (6th ed. 2015) ("modern liability policies typically include a distinct coverage part for *advertising injury* caused by an offense committed both during the policy period and in the course of advertising the insured's goods or services") (emphasis added); *see also* Hyundai Motor Am. v. Nat'l Union Fire Ins. Co., 600 F.3d 1092, 1098 (9th Cir. 2010) (holding "advertising" means "widespread promotional activities usually directed to the public at large," but "does *not* encompass 'solicitation'") (citation omitted) (emphasis in original); Simply Fresh Fruit v. Cont'l Ins. Co., 94 F.3d 1219, 1223 (9th Cir. 1996) ("under the policy, the advertising activities must cause the injury—not merely expose it"); Lexmark Int'l, Inc. v. Transp. Ins. Co., 327 Ill. App. 3d 128, 137 (App. Ct. 1st Dist. 2001) (while there is no generally accepted definition of advertising activity in the context of "personal and advertising injury" insurance coverage, the court found it generally referred to "the widespread distribution of promotional material to the public at large"); Phx. Am., Inc. v. Atl. Mut. Ins. Co., 2001 WL 1649243, at *6 (Cal. Ct. App. Dec. 24, 2001) (unpublished) (court defined "advertising" for purposes of CGL insurance coverage as "the act of calling public attention to one's product through widespread promotional activities"); *see also* Air Eng'g, Inc. v. Indus. Air Power, LLC, 828 N.W.2d 565, 572 (Wis. Ct. App. 2013) (court defined an "advertising idea" as "an idea for calling public attention to a product or business, especially by proclaiming desirable qualities so as to increase sales or patronage").

54. *See, e.g.*, Ins. Servs. Office, Inc., Commercial General Liability Coverage Form CG 00 01 12 07, § V(14) (2008), *available at* LEXIS, ISO Policy Forms (indicating that both personal injury and advertising injury can arise from oral or written publication that violates a person's right to privacy); Am. Family Mut. Ins. Co. v. C.M.A. Mortg., Inc., 2008 U.S. Dist. LEXIS 30233, at *16 (S.D. Ind. Mar. 31, 2008) (covering "oral or written publication, *in any manner*, of material that violates a person's right of privacy"; the "in any manner" language "le[ft] no room for equivocation" in holding that the insurer had a duty to defend the underlying Fair Credit Report Act violation case based on a solicitation letter, including with respect to statutory damages) (emphasis added); *see also* Evanston Ins. Co. v. Gene by Gene Ltd., 155 F. Supp. 3d 706 (S.D. Tex. 2016) (granting judgment to insured and finding that insurer must provide defense under coverage for advertising injury and personal injury where company allegedly published results of customers' DNA tests without consent, despite allegation that breach violated Genetic Privacy Act).

55. *See* section 16:2.2[A]–[B], *infra*.

[A] Publication Requirement

Particularly where advertising is required for coverage, insurers have frequently challenged whether the event implicating coverage constitutes a "publication" of information.

The importance of the publication requirement was recently addressed in *Recall Total Information Management v. Federal Insurance Co.*, where the insured lost computer tapes containing sensitive information of thousands of its clients' employees.[56] In that case, the court held that there was no publication since the insured could not establish that the information contained on the lost tapes was ever accessed by anyone, which the court held is a "necessary prerequisite to the communication or disclosure of personal information."[57]

Where there is dissemination, however, the issue becomes how widely that information must be disseminated in order to constitute publication. A leading case in this area is *Netscape Communications Corp. v. Federal Insurance Co.*[58] There, the underlying complaint alleged that Netscape had intercepted and internally disseminated private online communications.[59] The court held that internal disclosures of intercepted computer information and communications triggered coverage because the policy language covered disclosure to "any" person or organization.[60] Therefore, even though the alleged disclosure was confined within the company, coverage was triggered.[61]

As illustrated by *Netscape*, the publication requirement has generally required a rather limited showing by those seeking coverage. While the cases are not uniform on this point, most courts hold that an insured need not disclose information widely or externally to satisfy the requirement of publication in cases involving data breaches or unauthorized disclosure of private information.[62] Courts have held

---

56. Recall Total Info. Mgmt. v. Fed. Ins. Co., 83 A.3d 664, 672–73 (Conn. App. Ct. 2014) (involving a CGL policy that covered "personal injury," which was defined as "injury, other than bodily injury, property damage or advertising injury, caused by an offense of . . . electronic, oral, written or other publication of material that . . . violates a person's right to privacy"), *aff'd*, 115 A.3d 458 (Conn. 2015).
57. *Id.*; *see also* Defender Sec. Co. v. First Mercury Ins. Co., 803 F.3d 327 (7th Cir. 2015) (no coverage for alleged secret recording of sales calls because the recording of a phone call, without more, is insufficient to constitute a publication).
58. Netscape Commc'ns Corp. v. Fed. Ins. Co., 343 F. App'x 271 (9th Cir. 2009).
59. *Id.* at 272.
60. *Id.*
61. *Id.*
62. *Compare Netscape*, 343 F. App'x at 271 (publication requirement of policy was satisfied where disclosures were internal to the company), Encore

that disclosure to a single person can satisfy the publication requirement for advertising injury coverage.[63] Even where a publication must be a dissemination to the "public," courts have found coverage in cases involving widely disseminated information, like sending thousands of fax advertisements,[64] or posting information to the

---

Receivable Mgmt., Inc. v. Ace Prop. & Cas. Ins. Co., 2013 U.S. Dist. LEXIS 93513, at *31 n.17 (S.D. Ohio July 3, 2013) (internal transmission of information within a corporation constitutes publication), Norfolk & Dedham Mut. Fire Ins. Co. v. Cleary Consultants, Inc., 958 N.E.2d 853 (Mass. App. Ct. 2011) (finding that an insured's alleged transmittal of an employee's private information to her co-workers constitutes "publication" under a standard CGL policy), Virtual Bus. Enters., LLC v. Md. Cas. Co., 2010 Del. Super. LEXIS 141 (Super. Ct. Apr. 9, 2010) (finding transmittal of letters to a handful of former clients constituted "publication"), Zurich Am. Ins. Co. v. Fieldstone Mortg. Co., 2007 U.S. Dist. LEXIS 81570, at *14 (D. Md. Oct. 26, 2007) ("Of the circuits to examine 'publication' in the context of an 'advertising injury' provision, the majority have found that the publication need not be to a third party.") (citation omitted), *and* Tamm v. Hartford Fire Ins. Co., 16 Mass. L. Rep. 535 (Super. Ct. July 10, 2003) (accessing private emails and discussing contents with three people constituted publication for purposes of CGL coverage), *with* OneBeacon Am. Ins. Co. v. Urban Outfitters, Inc., 625 F. App'x 177, 180 (3d Cir. 2015) ("'publication' requires dissemination to the public"), Beard v. Akzona, Inc., 517 F. Supp. 128, 133 (E.D. Tenn. 1981) (finding that disclosure to only five persons was not sufficient to constitute publication), *and* C.L.D. v. Wal-Mart Stores, Inc., 79 F. Supp. 2d 1080, 1082–84 (D. Minn. 1999) (finding disclosure to three people insufficient publicity to warrant a claim for invasion of privacy).

63. *See, e.g.*, Zurich Am. Ins. Co. v. Fieldstone Mortg. Co., 2007 U.S. Dist. LEXIS 81570, at *17 (D. Md. Oct. 26, 2007) (holding that sending a person's credit report back to that particular person in the form of a prescreened letter for a mortgage constituted publication); Pietras v. Sentry Ins. Co., 2007 U.S. Dist. LEXIS 16015, at *9–10 (N.D. Ill. Mar. 6, 2007) (recognizing that publication of a consumer's credit information back to that one particular consumer can constitute publication); Motorist Mut. Ins. Co. v. Dandy-Jim, Inc., 912 N.E.2d 659, 666 (Ohio Ct. App. 2009) (insured's publication need not be made to person other than one whose privacy rights were violated); Hill v. MCI WorldCom Commc'ns, Inc., 141 F. Supp. 2d 1205, 1213 (S.D. Iowa 2001) (communication to one person constituted publicity due to confidential relationship between plaintiff and third party).

64. Penzer v. Transp. Ins. Co., 29 So. 3d 1000 (Fla. 2010) (finding coverage where sending thousands of unsolicited fax advertisements fit the "broad definition of 'publication' because it constitutes a communication of information disseminated to the public and it is 'the act or process of issuing copies . . . for general distribution to the public'"); Valley Forge Ins. Co. v. Swiderski Elecs., Inc., 860 N.E.2d 307 (Ill. 2006) (finding coverage where faxing unsolicited advertisements fit plain and ordinary sense of the word "publication" "both in the general sense of communicating information to the public and in the sense of distributing copies of the advertisements to the public"), *aff'd*, 2016 WL 1399517 (4th Cir. Apr. 11, 2016).

Internet regardless of whether there is any evidence that the posting was actually read.[65]

At least one court has held that disclosure to a recording device can constitute publication.[66] Although the publication requirement has been interpreted to apply to a broad range of potential disclosures,[67] some courts still require a definable disclosure to a party other than the person alleging the unauthorized disclosure.[68]

In a terse unpublished opinion,[69] a New York state court potentially added an additional perspective to the publication requirement. The court held that there was no coverage under a policy's personal and advertising injury provision for lawsuits related to a breach of data belonging to users of the company's online gaming product.[70] The court concluded that the CGL policy only provides coverage for publication of information *by the policyholder* and because hackers—not the company—had published the personal information at issue,

---

But see Defender Sec. Co. v. First Mercury Ins. Co., 803 F.3d 327 (7th Cir. 2015) (no coverage for alleged secret recording of sales calls because the recording of a phone call, without more, is insufficient to constitute a publication).

65. Travelers Indem. Co. of Am. v. Portal Healthcare Sols., LLC, 35 F. Supp. 3d 765 (E.D. Va. 2014) (holding that "[p]ublication occurs when information is 'placed before the public,' not when a member of the public reads the information placed before it").

66. *See* Encore Receivable Mgmt. v. Ace Prop. & Cas. Ins. Co., 2013 U.S. Dist. LEXIS 93513, at *29 (S.D. Ohio July 3, 2013) (finding publication by call center recording of conversation without consent); *see also* Complaint, InterContinental Hotels Grp. Res., Inc. v. Zurich Am. Ins. Co., No. 14-cv-04779-YGR (N.D. Cal. Oct. 27, 2014) (seeking a declaration of coverage for underlying putative class action alleging that the insured recorded customer service calls in violation of California's Invasion of Privacy Act).

67. *See* notes 62–63, *supra*, and 91–93, *infra*. *But see infra* note 68.

68. *See* Creative Hospitality Ventures, Inc. v. E.T. Ltd., Inc., 444 F. App'x 370 (11th Cir. 2011) (issuance of a receipt containing sensitive credit card information to a customer did not constitute publication, because it did not involve "dissemination of information to the general public"); Whole Enchilada Inc. v. Travelers Prop. Cas. Co. of Am., 581 F. Supp. 2d 677 (W.D. Pa. 2008) (personal and advertising injury provisions of policy were not triggered by alleged violations of the Fair and Accurate Credit Transactions Act where credit card numbers were printed on sales receipts and handed back to the customers themselves); *see also* Defender Sec. Co. v. First Mercury Ins. Co., 803 F.3d 327 (7th Cir. 2015) (no coverage for alleged secret recording of sales calls because the recording of a phone call, without more, is insufficient to constitute a publication). *But see* note 63, *supra*.

69. Zurich Am. Ins. Co. v. Sony Corp. of Am., 2014 N.Y. Misc. LEXIS 5141 (Sup. Ct. Feb. 21, 2014); *see also* note 72, *infra*.

70. *Id*.

there was no coverage.[71] The policyholder appealed the trial court's ruling, but two months after a New York appeals panel heard the appeal, the case settled without a ruling.[72]

[B] Right to Privacy As an Enumerated Offense

While the contours of the publication requirement appear relatively settled, many policies, particularly in recent years, do not include violation of a right to privacy as an enumerated offense or, where they do, have other exclusions that preclude coverage for data breaches.[73] Absent inclusion of infringement of a right to privacy as an enumerated offense, the advertising and personal injury sections of most CGL policies may not provide coverage for data theft or breach. Even where infringement of a right to privacy is included as an enumerated offense, insurers and insureds have often had vigorous disputes with respect to whether these provisions encompass data breaches.

In general, courts have explained that the right to privacy contains two distinct rights—the right to seclusion and the right to secrecy.[74] Some courts have used this distinction to conclude that only claims associated with a right to secrecy are insured under policy provisions covering personal and advertising injury.[75] However, others find that any ambiguity associated with the concept of a "right to privacy" in

---

71. *Id*.

72. Young Ha, *Sony, Zurich Reach Settlement in PlayStation Data Breach Case in New York*, INS. J., May 1, 2015, www.insurancejournal.com/news/east/2015/05/01/366600.htm.

73. *See, e.g.*, ISO Form CG 00 01 10 01 (2008) (excluding violation of right to privacy as an enumerated offense), quoted in note 16, *supra*; Business Liability Coverage Form BP 0100 01 04, Additional Exclusions § 2 (2004), IRMI.com, www.irmi.com/online/frmcpi/sc0000bp/chaaisbp/01000104.pdf (excludes from policy coverage any direct or indirect loss or loss of use caused by a computer virus or computer hacking).

74. *See, e.g.*, Pietras v. Sentry Ins. Co., No. 06 C 3576, 2007 U.S. Dist. LEXIS 16015, at *7–8 (N.D. Ill. Mar. 6, 2007) (privacy interests in seclusion and secrecy are both implicated by a "right to privacy"); ACS Sys., Inc. v. St. Paul Fire & Marine Ins. Co., 53 Cal. Rptr. 3d 786 (Ct. App. 2007) (CGL policy covers liability for violations of a privacy right of "secrecy" and not a privacy right of seclusion).

75. *See, e.g.*, Md. Cas. Co. v. Express Prods., 2011 U.S. Dist. LEXIS 108048, at *53 (E.D. Pa. Sept. 22, 2011) (concluding the right to secrecy the only right protected under "personal and advertising injury" of the CGL policies); ACS Sys., Inc. v. St. Paul Fire & Marine Ins. Co., 53 Cal. Rptr. 3d 786 (Ct. App. 2007) (a CGL policy covers liability for violations of a privacy right of "secrecy" and not a privacy right of seclusion); Res. Bankshares Corp. v. St. Paul Mercury Ins. Co., 407 F.3d 631 (4th Cir. 2005) (fax advertisements implicate a privacy right of seclusion, while CGL policy coverage relates only to "secrecy" privacy); *see also* note 81, *infra*, and accompanying text.

CGL coverage is reason to apply a broad definition covering both types of violations.[76]

Three types of insurance claims that have been heavily litigated under the personal and advertising provisions of CGL policies involve violations of the Telephone Consumer Protection Act (TCPA),[77] the Fair Credit Reporting Act[78] (FCRA), and state statutes precluding dissemination of ZIP codes.[79]

[B][1] Telephone Consumer Protection Act Cases

Cases asserting violations of the TCPA often involve the sending of unsolicited fax advertisements to third-party fax machines[80] or, more recently, unsolicited text messages to cellular phones.[81] In fax blast

---

76. *See* Owners Ins. Co. v. European Auto Works, Inc., 695 F.3d 814, 821 (8th Cir. 2012) ("The policies' reference to violating a 'right of privacy' thus encompasses the intrusion on seclusion caused by a TCPA violation for sending unsolicited fax advertisements[.]"); *Pietras*, 2007 U.S. Dist. LEXIS 16015 ("right to privacy" implicates both seclusion and secrecy); Penzer v. Transpor. Ins. Co., 29 So. 3d 1000 (Fla. 2010) (plain meaning of "right to privacy" includes any claim for privacy—whether involving a right to secrecy or seclusion); Park Univ. Enters. v. Am. Cas. Co., 442 F.3d 1239 (10th Cir. 2006) (holding that the dual meaning of the word "privacy" created an ambiguity in the policy and that it was reasonable to construe "privacy" to include the right to seclusion); State Farm Fire & Cas. Co. v. Kapraun, 2014 Mich. App. LEXIS 1276 (Ct. App. July 3, 2014) (rejecting insurer's argument that "'right of privacy' should be limited to the contours of Michigan tort law and, further, should only encompass a person's right to secrecy").
77. Telephone Consumer Protection Act of 1991 (TCPA), 47 U.S.C. § 227 (2010), discussed in section 16:2.2[B][1], *infra*.
78. Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681 *et seq.*, discussed in section 16:2.2[B][2], *infra*.
79. *See, e.g.*, OneBeacon Am. Ins. Co. v. Urban Outfitters, Inc., 625 F. App'x 177 (3d Cir 2015), discussed in section 16:2.2[B][3], *infra*.
80. The Illinois Supreme Court recently issued a significant decision on coverage of violations under the TCPA. Standard Mut. Ins. Co. v. Lay, 989 N.E.2d 591 (Ill. 2013). In that case, the insurer denied coverage for the insured's underlying TCPA action, arguing that the "TCPA-prescribed damages of $500 per violation constitute punitive damages, which 'are not insurable as a matter of Illinois law and public policy.'" *Id*. at 595. However, the court held that TCPA damages are not punitive, reasoning that the statute's purpose was "clearly" remedial in nature. *Id*. at 599–600. On remand, the Illinois Appellate Court held that the insurer must provide coverage to the insured for a settlement in a TCPA suit. Standard Mut. Ins. Co. v. Lay, 2 N.E.3d 1253 (Ill. App. Ct. 2014), *leave to appeal denied by* Standard Mut. Ins. Co. v. Lay, No. 117110, 2014 Ill. LEXIS 433 (Mar. 26, 2014). For further discussion of the *Lay* decision, see *infra* section 16:3.2[G], Definition of Loss.
81. *See, e.g.*, L.A. Lakers, Inc. v. Fed. Ins. Co., 2015 U.S. Dist. LEXIS 62159 (C.D. Cal. Apr. 17, 2015) (holding invasion of privacy exclusion applied to

cases, the distinction between the right to seclusion and the right to secrecy has been used to deny coverage where there was found to be a violation of one's right to seclusion, but not of the right to secrecy.[82] Under the cases where the right to seclusion is violated by way of unsolicited faxes or text messages, but there is no accompanying violation of one's interest in the secrecy of personal information, some courts hold there has been no violation of the right to privacy for insurance policy purposes.[83] Other courts have stated that the term "privacy" is ambiguous and can be read to include both a right to secrecy and a right to seclusion.[84] Under this latter view, any violation of a privacy right would implicate coverage.

Many policies have begun to explicitly exclude violations of certain statutory actions as a result of this broadened judicial interpretation of coverage for personal injury offenses based on the right of privacy.[85] Even here, courts have come to different conclusions as to whether

---

bar coverage stemming from sending unsolicited text messages), *appeal pending*; Doctors Direct Ins., Inc. v. Bochenek, 38 N.E.3d 116 (Ill. App. Ct. 1st Dist. 2015) (holding no coverage for class action involving text messages under cyber claims endorsement of professional liability policy because claims not based on a privacy wrongful act); Nat'l Union Fire Ins. Co. of Pittsburgh, Pa. v. Papa John's Int'l, Inc., 2014 U.S. Dist. LEXIS 90792 (W.D. Ky. July 3, 2014) (finding no coverage for unsolicited text messages sent in violation of the TCPA); *see also* Press Release, Fed. Commc'ns Comm'n, FCC Strengthens Consumer Protections Against Unwanted Calls and Texts (June 18, 2015), http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0619/DOC-333993A1.pdf (announcing increased protection under the TCPA against unwanted robo-calls and spam texts).

82. *See* Cynosure, Inc. v. St. Paul Fire & Marine Ins. Co., 645 F.3d 1 (1st Cir. 2011) (holding that the policy referred unambiguously to "disclosure" of private third-party information, and not to "intrusion"; therefore the policy did not cover claims for the mere receipt of faxes); Res. Bankshares Corp. v. St. Paul Mercury Ins. Co., 407 F.3d 631 (4th Cir. 2005) (finding that fax advertisements implicate a privacy right of seclusion, while CGL policy coverage relates only to "secrecy" privacy); ACS Sys., Inc. v. St. Paul Fire & Marine Ins. Co., 53 Cal. Rptr. 3d 786 (Ct. App. 2007) (holding that advertising injury provisions of a CGL policy did not cover ACS's liability for sending unsolicited fax advertisements because the policy covered only privacy right of "secrecy" and not a privacy right of seclusion); *see also* notes 75–76, *supra*, and accompanying text.

83. *See id.*; *see also L.A. Lakers*, 2015 U.S. Dist. LEXIS 62159; *Doctors Direct*, 38 N.E.3d 116.

84. *See* note 76, *supra*.

85. Commercial General Liability Form CG 00 01 12 07, Section I, Coverage B § (2)(P) (2008), *available at* LEXIS, ISO Policy Forms (excludes from coverage "Distribution of Materials in Violation of Statutes"). In November 2013, ISO made available a new endorsement entitled "Access or Disclosure of Confidential or Personal Information and Data Related Liability—with Limited Bodily Injury Exception." Ins. Servs. Office, Inc., Commercial General Liability Form CG 21 07 05 14 (2013), *available at*

exclusions related to the violation of various statutes actually apply to bar coverage.[86] Even in cases where statutory exclusions have been held to bar insurance for statutory claims, courts sometimes allow coverage for causes of action that would exist in the absence of the relevant statute.[87]

LEXIS, ISO policy forms (excluding coverage for "damages arising out of: (1) any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information, or any other type of nonpublic information; (2) or loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data"); *see also* Nat'l Union Fire Ins. Co. v. Coinstar, Inc., 2014 U.S. Dist. LEXIS 31441, at *5 (W.D. Wash. Feb. 28, 2014) (policy contained an exclusion relating to the violation of statutes banning the sending, transmitting, or communicating any material or information); Nationwide Mut. Ins. Co. v. Harris Med. Assocs., LLC, 973 F. Supp. 2d 1045, 1050 (E.D. Mo. Sept. 23, 2013) (insurance policy contained a Violation of Consumer Protection Statutes exclusion for "'any action or omission that violates or is alleged to violate' the TCPA, or any 'statute . . . that addresses, prohibits or limits the electronic printing, dissemination, disposal, sending, transmitting, communicating or distribution of material or information'"); G.M. Sign, Inc. v. State Farm Fire & Cas. Co., 18 N.E.3d 70, 74 (Ill. Ct. App. 2014) ("Distribution of Material in Violation of Statutes Exclusion" applied to "Bodily injury, property damage, personal injury, or advertising injury *arising directly or indirectly out of* any action or omission that violates or is alleged to violate [t]he Telephone Consumer Protection Act (TCPA)."") (emphasis added).

86. *Compare* Evanston Ins. Co. v. Gene by Gene Ltd., 155 F. Supp. 3d 706 (S.D. Tex. 2016) (policy excluded violations of TCPA, CAN-SPAM, and any other statute that "prohibits or limits the sending, transmitting, communication or distribution of information or other material," but it did not apply to bar coverage of Alaska Genetic Privacy Act claims), Hartford Cas. Ins. Co. v. Corcino & Assocs., 2013 U.S. Dist. LEXIS 152836 (C.D. Cal. Oct. 7, 2013) (holding that the statutory exclusion for "Personal And Advertising Injury . . . [a]rising out of the violation of a person's right to privacy created by any state or federal act" did not apply to bar coverage for the insured hospital's data breach because at common law, medical records have long been deemed confidential and private, and because the legislative history of the relevant statutes shows that they were not enacted to create new privacy rights), *with* Scottsdale Ins. Co. v. Stergo, 2015 U.S. Dist. LEXIS 127268 (N.D. Ill. Sept. 23, 2015) (holding that the exclusion for "violation of statutes that govern emails, fax, phone calls or other methods of sending material or information" barred coverage for sending unsolicited junk fax advertisements), Nat'l Union Fire Ins. Co. v. Coinstar, Inc., 2014 U.S. Dist. LEXIS 31441 (W.D. Wash. Feb. 28, 2014) (holding that the "Violation of Statutes in Connection with Sending, Transmitting, or Communicating Any Material Or Information" exclusion applied to bar coverage when the plaintiffs alleged a violation of the Video Protection Privacy Act).

87. *See, e.g.*, Hartford Cas. Ins. Co. v. Corcino & Assocs., 2013 U.S. Dist. LEXIS 152836, at *11 (C.D. Cal. Oct. 7, 2013) (stating that the statutory

[B][2] Fair Credit Reporting Act Cases

While fax blast cases may raise special issues about whether there is an invasion of a right to seclusion or a right to secrecy, FCRA cases typically involve disclosures of personal information that is asserted to be confidential. A leading case in this area is the decision of the federal court in *Zurich American Insurance Co. v. Fieldstone Mortgage Co.*[88] In that case, a mortgage company was alleged to have improperly accessed and used individual credit information, in violation of the FCRA, in order to provide "pre-screened" offers of mortgage services.[89] The insurer denied coverage for the resulting claims.[90] The court noted that the FCRA was enacted to ensure the protection of privacy rights and held that the insurer had a duty to defend against the FCRA claims because they fell under the "personal and advertising injury coverage" of the insured's CGL policy.[91]

Like many privacy-related cases, coverage in the *Fieldstone Mortgage* case turned on whether the FCRA claim alleged a violation of a "right to privacy" and whether there had been publication of the information at issue. In analyzing the scope of the publication requirement to assess coverage, the court explicitly rejected the insurance company's argument that "in order to constitute publication, the information that violates the right to privacy must be divulged to a third party."[92] Noting that a majority of circuits have rejected this argument,[93] the court held that publication need not be to

---

exclusion would not apply to damages alleged that would have occurred in the absence of the statutes); Nationwide Mut. Ins. Co. v. Harris Med. Assocs., LLC, 973 F. Supp. 2d 1045 (E.D. Mo. 2013) (holding that the Violation of Statues exclusion did not negate the potential for coverage for common claims); Axiom Ins. Managers, LLC v. Capitol Specialty Ins. Corp., 876 F. Supp. 2d 1005, 1015 (N.D. Ill. 2012) (holding that the Distribution of Material exclusion did not exclude coverage of common law claim). *But see* Big 5 Sporting Goods Corp. v. Zurich Am. Ins. Co., 635 F. App'x 351, 353–54 (9th Cir. 2015) (holding that common law claims that were not separate and apart from any statute violations were subject to the statutory exclusions); CE Design Ltd. v. Cont'l Cas. Co., 2016 WL 2342858 (Ill. App. Ct. May 2, 2016) (holding no coverage for common law claims because they arose from the same conduct that was the basis for the TCPA claim); Ill. Cas. Co. v. W. Dundee China Palace Rest., Inc., 49 N.E.3d 420 (Ill. App. Ct. 2015) (holding that there was no coverage because common law claims were merely a "rephrasing" of the TCPA conduct).

88. Zurich Am. Ins. Co. v. Fieldstone Mortg. Co., 2007 U.S. Dist. LEXIS 81570 (D. Md. Oct. 26, 2007).
89. *Id.* at *2.
90. *Id.* at *4.
91. *Id.* at *9, *11.
92. *Id.* at *14 (citing Park Univ. Enters. v. Am. Cas. Co., 442 F.3d 1239, 1248–49, 1250 (10th Cir. 2006)).
93. *Id.*; *see also* notes 62–68, *supra*.

a third party and that unauthorized access and use was all that was necessary to violate a privacy right for coverage purposes.[94]

[B][3] "ZIP Code" Cases

Another area of recent litigation has concerned the gathering of ZIP codes and personal information at the time of credit card purchases. A number of states have statutes that arguably relate to these practices, and several consumer class actions have been brought pursuant to these statutes or common law.[95] For example, in *One Beacon American Insurance Co. v. Urban Outfitters*, the court rejected one of the insured's claims for coverage on the ground that there was no allegation of public dissemination of information and publication required communication to the public at large.[96] A second claim was rejected on the theory that receipt of unsolicited junk mail alleged a violation of the right to seclusion, not secrecy, and was therefore not within the right of privacy covered by the policy.[97] While it found that a third claim was sufficiently disseminated to satisfy the publication requirement, the court nonetheless held that coverage was precluded by a statutory exclusion against collecting or recording information.[98] A similar exclusion was applied by the court in *Big 5 Sporting Goods Corp. v. Zurich American Insurance Co.*,[99] which also refused to find a common law claim outside the exclusion.[100]

---

94. *Zurich Am. Ins. Co.*, 2007 U.S. Dist. LEXIS 81570, at *14, *17–18.
95. *See, e.g.*, OneBeacon Am. Ins. Co. v. Urban Outfitters, Inc., 625 F. App'x 177 (3d Cir. 2015); Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co., 691 F.3d 821 (6th Cir. 2012).
96. *OneBeacon*, 625 F. App'x at 180 (requiring publication to be to the "public at large"). *But see supra* notes 62–63.
97. *See id*. at 182.
98. *Id*. at 181–82 (citing the "Recording and Distribution of Material or Information in Violation of Law Exclusion," which excluded "'Personal and advertising injury' arising directly or indirectly out of any action or omission that violates or is alleged to violate . . . [any] statute, ordinance or regulation . . . that addresses, prohibits or limits the . . . dissemination, . . . collecting, recording, sending, transmitting, communicating or distribution of material or information."). *But see supra* notes 62–63 and 86–87.
99. Big 5 Sporting Goods Corp. v. Zurich Am. Ins. Co., 635 F. App'x 351, 353 (9th Cir. 2015) (applying the distribution of material in violation of statutes exclusion to coverage for "'[p]ersonal and [a]dvertising [i]njury' arising directly or indirectly out of any action or omission that violates or is alleged to violate: [a]ny 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"), *aff'g* 957 F. Supp. 2d 1135 (C.D. Cal. 2013). *But see supra* notes 86–87.
100. 957 F. Supp. 2d at 1151 (holding that because the relevant privacy right was not based on common law and created by statute, coverage for the common law claim was barred by the distribution of material exclusion).

§ 16:2.3 Other Coverages

While most companies seeking coverage under traditional policy forms will assert claims under first-party property or third-party CGL policies, policyholders may also seek coverage for data or privacy breaches under other contracts in their insurance portfolio including D&O insurance, E&O policies, and Commercial Crime Policies.

[A] Directors and Officers Liability Insurance

D&O insurance is generally designed to cover losses arising from claims made during the policy period that allege wrongs committed by "directors and officers."[101] As such, this type of insurance may be limited to circumstances where an officer or director is sued directly in connection with a privacy breach—perhaps for lack of supervision or personal involvement in dissemination of confidential information.

Some D&O policies, and similar policies available to not-for-profits or companies that are not publicly traded, also contain "entity" coverage, which provides insurance for certain claims against the entity itself. In many instances, "entity" coverage is limited to securities claims,[102] but this is not always the case. Where entity coverage is broad, it may encompass liabilities for privacy breaches and other cyber risks.

The relevance of D&O coverage with respect to cyber issues increased significantly in 2014 and 2015 as shareholder derivative actions were filed against officers and directors of Target[103] and Wyndham[104] as a result of widely reported cyber breaches involving those companies. These lawsuits challenge the level of supervision by board members

---

101. *See, e.g.*, PLM, Inc. v. Nat'l Union Fire Ins. Co., 1986 U.S. Dist. LEXIS 17014, at *6–7 (N.D. Cal. Dec. 2, 1986) (policy provided coverage to individual directors and officers for loss incurred in their capacity as directors and officers), *aff'd*, 848 F.2d 1243 (9th Cir. 1988); Sphinx Int'l, Inc. v. Nat'l Union Fire Ins. Co., 412 F.3d 1224, 1227–28 (11th Cir. 2005) (policy providing coverage for duly elected directors and officers for loss incurred in their capacity as directors and officers). *See generally* 4 DAN A. BAILEY ET AL., NEW APPLEMAN ON INSURANCE § 26.01 (2015).

102. *See, e.g.*, D&O Insuring Agreements, IRMI.com, www.irmi.com/online/pli/ch010/1l10e000/al10e010.aspx#jd_entity_securities_coverage_side_c (last visited June 23, 2014) ("the vast majority of D&O policies that provide entity coverage do so *only* as respects securities claims").

103. *See In re* Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482, 490 (D. Minn. 2015) (granting motion for class certification).

104. *See* Complaint, Palkon v. Holmes, No. 2:14-cv-01234 (D.N.J. Feb. 25, 2014); *see also* Palkon v. Holmes, 2014 WL 5341880 (D.N.J. Oct. 20, 2014) (finding that board's decision not to bring suit against the company for inadequate data security was not in violation of the business judgment rule, reasoning that the board took adequate steps to familiarize itself with the subject matter of the demand and that it had ample information at its disposal).

and claim that they "failed to take reasonable steps to maintain their customers' personal and financial information in a secure manner."[105] These kinds of claims and increasing public attention to these issues[106] underscore the importance of D&O coverage and careful board vigilance in relation to data retention, cybersecurity, and relevant insurance coverage. They also emphasize the importance of avoiding overbroad cyber exclusions in D&O policies so that normal D&O exposures are not excluded simply because they may relate to cybercrimes.[107]

[B] Errors and Omission Policies

E&O policies provide coverage for claims arising out of the rendering of professional services.[108] Such policies may provide coverage for data breaches or privacy-related claims that arise from the "rendering of services" so long as policy definitions and exclusions do not exclude losses relating to such breaches or Internet-related services.[109] E&O

---

105. *See* Complaint, Palkon v. Holmes, No. 14-cv-01234 (D.N.J. Feb. 25, 2014); *see also In re* Heartland Payment Sys., Inc. Sec. Litig., 2009 WL 4798148, at *2, *8 (D.N.J. Dec. 7, 2009) (dismissing suit where plaintiffs alleged that the defendants falsely represented that the company "place[d] significant emphasis on maintaining a high level of security" and maintained a network that "provide[d] multiple layers of security to isolate [its] databases from unauthorized access").

106. Danny Yadron, *Corporate Boards Race to Shore up Cybersecurity*, WALL ST. J., June 29, 2014, http://online.wsj.com/articles/boards-race-to-bolster-cybersecurity-1404086146. In a June 10, 2014, speech, SEC Commissioner Luis Aguilar emphasized that "ensuring the adequacy of a company's cybersecurity measures needs to be a part of a board of director's risk oversight responsibilities." Luis A. Aguilar, Comm'r, U.S. Sec. & Exch. Comm'n, Speech at the Cyber Risks and the Boardroom Conference: Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus (June 10, 2014).

107. *See also infra* note 214.

108. *See, e.g.*, Pac. Ins. Co. v. Burnet Title, Inc., 380 F.3d 1061, 1062 (8th Cir. 2004) ("Pacific issued an Errors and Omissions (E&O) insurance policy . . . which provided coverage for negligent acts, errors, or omissions in the rendering of or failure to render professional services."); Matthew T. Szura & Co. v. Gen. Ins. Co. of Am., 543 F. App'x 538, 540–41, 543 (6th Cir. 2013) (holding that the E&O policy at issue covered "wrongful acts arising out of the performance of professional services for others," but not "intentionally wrongful conduct"). *See generally* 4 PAUL S. WHITE & RICHARD L. NEUMEIER, APPLEMAN ON INSURANCE § 25.01 (2012).

109. *See, e.g.*, Eyeblaster, Inc. v. Fed. Ins. Co., 613 F.3d 797 (8th Cir. 2010) (in addition to finding coverage for property damage under a CGL policy, the court found that coverage existed under an E&O policy, stating that the definition of "error" in a technology errors and omissions policy included intentional, non-negligent acts but excludes intentionally wrongful conduct). *But see* Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., Inc.,

policies designed for medical professionals or health plan fiduciaries often include specific coverages for HIPAA and other privacy exposures, including computer privacy breaches.[110]

Attorney and other malpractice policies may also cover certain risks associated with unintentional release of confidential information or client funds. For example, in *Stark & Knoll Co. L.P.A. v. ProAssurance Casualty Co.*,[111] the court held that the insured law firm may be covered under its malpractice policy when one of its attorneys fell victim to an alleged phishing scam and sent nearly $200,000 of client funds to an offshore account.[112]

Law firms have become repeated targets of cyber attacks seeking confidential client information about transactional and other matters.[113] These kinds of matters may give rise to asserted claims for improper protection of client information.[114]

2015 WL 2201797 (D. Utah May 11, 2015) (holding there was no duty to defend under the insured's CyberFirst Policy since the policy covered an "error, omission or negligent act" and the underlying lawsuit alleged that the insured intentionally refused to return the plaintiff's customer data); Margulis v. BCS Ins. Co., 23 N.E.3d 472 (Ill. App. Ct. 1st Dist. 2014) (holding that automated telephone calls advertising insured's business did not constitute negligent acts, errors or omissions by insured in "rendering services for others" since the insured was not rendering services for the call recipients).

110. *See, e.g.*, Med. Records Assocs., Inc. v. Am. Empire Surplus Lines Ins. Co., 142 F.3d 512, 516 (1st Cir. 1998) (in coverage dispute case, court noted that hospital employees involved in safeguarding personal medical information may have coverage under an E&O policy given the substantial "risks associated with release of records to unauthorized individuals"); Princeton Ins. Co. v. Lahoda, D.C., 1996 WL 11353 (E.D. Pa. Jan. 4, 1996) (finding an improper disclosure of confidential patient information was covered by a professional liability insurance policy).

111. Stark & Knoll Co. L.P.A. v. ProAssurance Cas. Co., 2013 U.S. Dist. LEXIS 50326 (N.D. Ohio Apr. 8, 2013).

112. *Id*. at *3, *9–23; *see also* Nardella Chong, P.A. v. Medmarc Cas. Ins. Co., 642 F.3d 941 (11th Cir. 2011) (losses due to Nigerian check scam arose from provision of professional services and were covered by attorney's professional liability insurance policy); note 117, *infra*. *But see* Attorneys Liab. Prot. Soc'y, Inc. v. Whittington Law Assocs., PLLC, 961 F. Supp. 2d 367, 375 (D.N.H. 2013) (holding that "the plain and unambiguous language" of policy exclusion "for any claim arising from or in connection with any conversion, misappropriation or improper commingling" excludes coverage for misappropriation of funds).

113. Jason Bloomberg, *Cybersecurity Lessons Learned From "Panama Papers" Breach*, FORBES (Apr. 21, 2016), www.forbes.com/sites/jasonbloomberg/2016/04/21/cybersecurity-lessons-learned-from-panama-papers-breach/#4042b98b4f7a.

114. Gabe Friedman, *Threats of Litigation After Data Breaches at Major Law Firms*, BLOOMBERG LAW (Mar. 30, 2016).

[C] Crime Policies

Crime policies generally provide first-party coverage and insure a policyholder's property against theft.[115] In some cases, crime policies also provide third-party coverage against an insured's liability for theft, forgery, or certain other crimes injuring a third party.[116] Insureds are increasingly turning to this coverage in cases involving theft resulting from the inadvertent transferring of funds caused by a fraudulent email.[117]

While the courts have recognized that the concept of a crime policy seems on its face to encompass theft of confidential information, many crime policies specifically exclude theft of cyber or intellectual property.[118] Even when this is not the case, these

---

115. *See, e.g.*, Medidata Sols., Inc. v. Fed. Ins. Co., No. 1:15-cv-00907 (S.D.N.Y. Mar. 10, 2016) (rejecting cross-motions for summary judgment on computer fraud policy in coverage action for phishing scam perpetrated against medical data services provider); Universal Am. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa., 37 N.E.3d 78 (N.Y. 2015) (denying coverage under policy's computer fraud section for Medicare fraud scheme perpetrated by employees, reasoning that use of computer to make false entries about medical treatments that were never provided was merely incidental to fraud scheme).

116. *See, e.g.*, Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co., 691 F.3d 821 (6th Cir. 2012) (affirming the district court's grant of summary judgment for the insured and upholding ruling under Ohio law that a commercial crime policy, which included a computer and funds transfer fraud endorsement, covered third-party costs resulting from data breach and hacking attack).

117. *See, e.g.*, Apache Corp. v. Great Am. Ins. Co., 2015 WL 7709584 (S.D. Tex. Aug. 7, 2015) (appeal pending) (finding coverage under insured's crime protection policy covering "computer fraud" for insured's inadvertent wire transfer of $1.4 million caused by a fraudulent email, reasoning that insured's loss resulted "directly from [computer fraud]"); State Bank v. BancInsure, Inc., 823 F.3d 456 (8th Cir. 2016) (finding coverage under insured's financial institution bond for fraudulent transfer caused by computer virus, reasoning that "the computer systems fraud was the efficient and proximate cause of [the] loss," regardless if other non-covered causes contributed); Ameriforge Grp., Inc. v. Fed. Ins. Co., No. 2016-00197 (Tex. Dist. Ct. Harris Cty. Jan. 4, 2016) (alleging that defendant breached its contract by denying coverage for inadvertent wire transfer prompted by fraudulent email).

118. *See, e.g.*, Cargill, Inc. v. Nat'l Union Fire Ins. Co., 2004 Minn. App. LEXIS 33, at *18 (Ct. App. Jan. 13, 2004) (crime policy specifically excluded "loss resulting directly or indirectly from the accessing of any confidential information, including, but not limited to, trade secret information, computer programs, confidential processing methods or other confidential information of any kind"); Ins. Servs. Office, Inc., Commercial Crime Coverage Form CR 00 20 05 06 § (F)(15) (2008), *available at* LEXIS, ISO Policy Forms (explicitly excludes computer programs and electronic data from the definition of "property"). *But see Retail Ventures*, 691 F.3d

policies often limit coverage to theft of physical things or cash or securities.[119]

§ 16:3 Modern Cyber Policies

While some specialized coverages, such as errors and omissions (E&O) insurance in the medical or fiduciary context, specifically include cyber and privacy risks inherent in the activity on which coverage is focused, as discussed above, traditional policy forms often impose significant limitations on coverage for these kinds of risks.[120] Indeed, it is likely that gaps in coverage for cyber and privacy risks will continue to widen as insurers increase the number of exclusions designed to limit coverage in traditional policies for these kinds of claims and try to confine coverage for cyber and privacy to policies specifically designed for this purpose.[121]

In response to the coverage gaps created by evolving exclusions and policy definitions, the market for cyber insurance policies has responded with a host of new policies.[122] The new policy offerings are typically named peril policies and offer coverage on a claims-made basis. However, because of the ever-evolving nature of the risks presented and the lack of standard policy terms, these offerings are in an ongoing state of flux as insurers continue to change and refine their policy forms. As a result, risk managers looking to purchase cyber insurance products have latitude to negotiate and should carefully evaluate the needs and risks for which coverage is sought against a

---

821 (finding coverage under computer fraud rider to blanket crime policy for losses from hacker's theft of customer credit card and checking account data).

119. *See, e.g.*, Ins. Servs. Office, Inc., Commercial Crime Coverage Form CR 00 20 05 06 § (A)3–8; § (F)(15) (2008) (coverage is for loss of money or securities, fraud, and theft of "other property," which is defined as "any tangible property other than 'money' and 'securities' that has intrinsic value" but excluding computer programs and electronic data).

120. *See* section 16:2, *supra*.

121. *See* notes 16, 29, 32, 47, 73, 85, and 119, *supra*.

122. *See, e.g., Travelers Knows Cyber Insurance*, TRAVELERS, www.travelers.com/business-insurance/cyber-security/index.aspx (last visited Aug. 17, 2016); CyberEdge, AIG, www.aig.com/CyberEdge_3171_417963.html; CHUBB CyberSecurity Form 14-02-14874, § I.J. (2009); Philadelphia Insurance Co. Cyber Security Liability Coverage Form PI-CYB-001, § I.C. (2010); *see also* RICHARD S. BETTERLY, THE BETTERLEY REPORT: CYBER/PRIVACY INSURANCE MARKET SURVEY 2015 (June 2015) (surveying over thirty carriers that offer cyber insurance products), http://betterley.com/samples/cpims15_nt.pdf.

detailed evaluation of the coverage actually provided by the new policy.[123]

§ 16:3.1 Key Concepts in Cyber Coverage

As noted above, two important features of cyber policies are that they are often named peril policies and written on a claims-made basis.

[A] Named Peril

Although the derision of all-risk and named-peril policies is based on conceptual frameworks that developed largely in the first-party context and many policies are hybrids that do not fall neatly in one category or the other, insurance policies are often categorized as either all-risk or named-peril policies.

All-risk policies typically cover all risks in a particular category unless they are expressly excluded. For example, the classic all-risk property policy covers "all risk of direct physical loss or damage" to covered property unless excluded.[124] These policies are said to offer broad and comprehensive coverage.[125]

Named-peril policies, on the other hand, cover only specified "perils" or risks. In the traditional property context, this may have been wind, storm, and fire, with some policies covering floods while others do not. Unlike all-risk policies, named-peril policies do not typically provide coverage for risks other than the named perils.[126]

---

123. A recent white paper published by Wells Fargo noted that survey respondents' biggest challenge to purchasing cyber coverage was finding a policy that fit the company's needs (47% of respondents). Dena Cusick, *2015 Cyber Security and Data Privacy Survey: How Prepared Are You?*, at 3 (Wells Fargo, White Paper Sept. 2015).

124. *See, e.g.*, City of Burlington v. Indem. Ins. Co. of N. Am., 332 F.3d 38, 47 (2d Cir. 2003) ("All-risk policies . . . cover all risks except those that are specifically excluded.").

125. *See, e.g.*, Villa Los Alamos Homeowners Ass'n v. State Farm Gen. Ins. Co., 130 Cal. Rptr. 3d 374, 382 (Ct. App. 2011) ("Coverage language in an all risk . . . policy is *quite broad*, generally insuring against all losses not expressly excluded."). *See generally* 7 COUCH ON INSURANCE § 101:7 (3d ed. 2011).

126. *See, e.g.*, Burrell Commc'ns Grp. v. Safeco Ins., 1995 U.S. Dist. LEXIS 11699, at *3 (N.D. Ill. Aug. 10, 1995) (the insurance policy at issue in the case was "an enumerated perils policy, meaning that only certain named perils are covered"). *See generally* 4 JEFFREY E. THOMAS, NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 29.01(3)(b)(1) (2015) ("'named peril' policies . . . cover only the damages that result from specific categories of risks, and 'all risks' policies . . . cover the damages from all risks except those specifically excluded by the policy").

Cyber policies are generally named-peril policies, at least in the first-party property context, and different carriers have used dramatically different policy structures and definitions to describe what they cover and what they do not. Some of the more typical areas of coverage include:

First-party coverages

- costs of responding to a data breach, including privacy notification expenses and forensics
- loss of electronic data, software, hardware, and costs of reconstructing data
- loss of use and business interruption
- data security and privacy injury
- loss from cyber crime
- rewards for responding to cyber threats and extortion paid
- business interruptions due to improper access to computer systems
- public relation for cyber risks

Third-party coverages

- suits against insured for data breach or defamation
- loss of another's electronic data, software or hardware, resulting in loss of use
- loss of funds of another due to improper transfer
- data security and privacy injury
- statutory liability under state and federal privacy laws
- advertising injury
- intellectual property infringement

Governmental action may fall in both first- and third-party covers depending on particular policy wording.

[B] Claims Made

Most cyber policies are claims-made policies, which in very general terms means that the policy is triggered by a claim made and, in some cases, noticed during the policy period.[127] Most claims-made policies

127. *See generally* 2 RONALD N. WEIKERS, DATA SEC. AND PRIVACY LAW § 14:36 (2015).

contain provisions, commonly known as "tail" provisions, which provide an extended reporting period during which an insured can give notice of a claim made after the end of the policy period that alleges a wrongful act before the policy period ended.[128] But even here, there is often a specific time span in which notice must be given to the insurer.[129]

Claims-made policies are distinguished from occurrence policies, which are typically triggered by an event or damage during the policy period, regardless of when the occurrence is known to the insured or notified to the insurer.[130] In some cases, such as mass torts, environmental contamination or asbestos, occurrence policies in effect at the time of the contamination or exposure to an allegedly dangerous product or substance can cover claims asserted decades later after the contamination is discovered or the policyholder is sued by a claimant who alleges recent diagnosis of illness.[131]

Because cyber policies usually are written on a claims-made basis, they generally cover claims made, and in some cases noticed, during the policy period. This allows the insurer to attempt to limit exposure to the policy period (and any tail period) without having to wait many years to see if a breach is later discovered to have occurred during the period the policy was in effect.

In addition to having dates by which notice must be given, many claims-made policies have "retro" dates that preclude claims for breaches prior to a designated date, regardless of when the claim is asserted and noticed to the insurer.[132] Often, these retro dates are

---

128. *See generally* 3 JEFFREY E. THOMAS, NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 16.07 (2012).

129. *See, e.g.*, Prodigy Commc'ns Corp. v. Agric. Excess & Surplus Ins. Co., 288 S.W.3d 374, 375 (Tex. 2009) (claims-made policy's tail provision required insured to give notice of a claim "as soon as practicable . . . , but in no event later than ninety (90) days after the expiration of the Policy Period" which the court found binding).

130. *See generally* 3 ALLAN D. WINDT, INSURANCE CLAIMS AND DISPUTES § 11.5 (6th ed. 2013).

131. *See, e.g.*, Scott's Liquid Gold, Inc. v. Lexington Ins. Co., 293 F.3d 1180, 1182–83 (10th Cir. 2002) (upholding a decision finding insurer has a duty to indemnify insured for occurrence of pollution into soil and groundwater in the 1970s, even though the action was brought in 1994); Keene Corp. v. Ins. Co. of N. Am., 667 F.2d 1034, 1040 (D.C. Cir. 1981) (finding insurer liable for injuries, as defined by the policy, that caused asbestos-related harm many years after inhalation in an occurrence policy). *See generally* 4 JEFFREY E. THOMAS, NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 27.01 (2015).

132. *See, e.g.*, Coregis Ins. Co. v. Blancato, 75 F. Supp. 2d 319, 320–21 (S.D.N.Y. 1999) ("'Retroactive Date' is defined in the policy as: the date, if specified in the Declarations or in any endorsement attached hereto, on or after which

designed to limit coverage to the first time a particular carrier began issuing claims-made policies to a particular insured.

Many policies also include provisions aggregating claims from a single breach or related series of breaches into one insurance contract or period in effect when the first claim is asserted.[133] In addition, it may be possible under some policy provisions to provide a notice of circumstance, which will bring claims asserted after the policy expires into the policy period when the notice of circumstances was asserted.[134] Such notices are often at the discretion of the insured, but insurers sometimes raise issues as to the level of particularity required for such notices to be effective.

§ 16:3.2 Issues of Concern in Evaluating Cyber Risk Policies

Though they vary in structure and form, the new cyber risk policies raise a variety of issues, some of which are akin to issues posed by more traditional insurance policies and some of which are unique to these new forms.

[A] What Is Covered?

As noted above, cyber policies are, at least in some respects, named-peril policies.[135] In other words, they generally cover specifically identified risks. In order to determine the utility of the coverage being provided, a policyholder needs to assess carefully its own risks and then compare them to the protections provided by a particular form. For example, a company in the business of providing cloud computing

---

any act, error, omission or PERSONAL INJURY must have occurred in order for CLAIMS arising therefrom to be covered under this policy. CLAIMS arising from any act, error, omission or PERSONAL INJURY occurring prior to this date are not covered by this policy."); City of Shawnee v. Argonaut Ins. Co., 546 F. Supp. 2d 1163, 1181 (D. Kan. 2008) (policy contains "a Retroactive Date-Claims Made Coverage endorsement"). *See generally* 3 JEFFREY E. THOMAS, NEW APPLEMAN INSURANCE LAW PRACTICE GUIDE § 16.07 (2015).

133. *See, e.g.*, WFS Fin. Inc. v. Progressive Cas. Ins. Co., 2005 U.S. Dist. LEXIS 46751, at *6 (C.D. Cal. Mar. 29, 2005) (policy stated: "Claims based upon or arising out of the same Wrongful Act or Interrelated Wrongful Acts committed by one or more of the Insured Persons shall be considered a single Claim, and only one Retention and Limit of Liability shall be applicable . . . each such single claim shall be deemed to be first made on the date the earliest of such Claims was first made, regardless of whether such date is before or during the Policy Period."), *aff'd*, 232 F. App'x 624 (9th Cir. 2007).

134. *See generally* 3 JEFFREY E. THOMAS, NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 20.01 (2015).

135. *See* section 16:3.1[A], *supra*.

services to third parties gains limited protection from a policy form that specifically excludes, or does not cover in the first place, liabilities to third parties due to business interruption.[136] On the other hand, a company that is highly reliant on cloud providers is left with substantial uninsured risk when its cyber policy does not include loss of information or disruption of its cloud provider. In another illustration of the issue, the array of problems and issues of policyholders that sell computer services are different from those of companies that sell no services to others but handle a great deal of statutorily protected medical or personal financial information. The first step in analyzing the cyber policy is to compare the risks of the policyholder at issue to the specific coverages provided.

[B] Confidential Information, Privacy Breach, and Other Key Definitions

Under most cyber policies, there are key definitions such as confidential information, personal identifiable information, computer or computer system, and privacy or security breach that are crucial to analyzing and understanding coverage. In some cases, policy language ties these definitions to statutory schemes in the United States and abroad that themselves are constantly changing.[137]

However they are drafted, these key definitions and their applicability can be very technical and need to be reviewed by both insurance and technology experts to ensure that the risks inherent in a particular technology platform are adequately covered. This is particularly true as more and more businesses rely on third-party providers or affiliated entities within a corporate family for technology services. For example, some policies may cover leased computers or information in the hands of vendors while other policies may not. Coverage for data in the hands of a third party may require memorialization of the relationship in a written contract. Careful vetting of these key definitions is essential to understanding and negotiating coverage.

---

136. In an example of insurance products evolving to meet specific needs, the International Association of Cloud & Managed Service Providers (MSPAlliance) recently announced that it had partnered with Lockton Affinity to offer a new Cloud and Managed Services Insurance Program, which offers "comprehensive protection for cloud and managed service providers (MSPs)." *See* Celia Weaver, *MSPAlliance® Launches Cloud Computing Insurance Program*, MSPALLIANCE (Apr. 25, 2013), http://mspalliance.com/mspalliance-launches-cloud-insurance-program/.

137. In 2015, thirty-three states introduced or considered revisions to their existing security breach laws. *2015 Security Breach Legislation*, NAT'L CONFERENCE OF STATE LEGISLATURES (Dec. 31, 2015), www.ncsl.org/research/telecommunications-and-information-technology/2015-security-breach-legislation.aspx.

[C] Overlap with Existing Coverage

One of the difficult issues with the new cyber policies is determining what coverage they provide in comparison to the insurance provided by traditional policies. Most risk managers do not want to pay for the same coverage twice, much less to have two carriers arguing with each other as to which is responsible, or about how to allocate responsibility between them for a particular loss.

Many brokers prepare analyses for their clients of the interplay between traditional coverages and cyber policies, and these comparisons should be considered carefully to avoid multiple and overlapping coverages for the same risks. Examples of potential overlaps may include: physical destruction to computer equipment covered by property and cyber policies; disclosure of confidential personal information potentially covered by CGL, E&O, and cyber policies; and theft of computer resources or information under crime and cyber policies. The extent of any overlap among these or other coverage may only be identified by careful analysis.

[D] Limits and Deductibles

Because cyber policies are typically structured as named peril policies, they often have specific limits or sublimits as well as deductibles for each type of coverage. Many cyber policies are crafted for "low frequency but high severity" cyber-attacks affecting large amounts of electronic data.[138] However, some companies now face a growing number of repeated smaller-scale data breaches and need to consider deductible structures that will permit coverage for these costs.[139] In any event, primary and excess limits associated with a particular coverage must be reviewed to ensure adequate coverage for risks of key concern.

One issue that often arises in traditional policies, and may also arise in the cyber context, is whether an insured's losses are subject to multiple sublimits or multiple deductibles. For example, an insured's policy may contain multiple "sublimits," or "per claim" or "per occurrence" deductibles[140] that apply to losses in various categories.[141]

---

138. *See* ADVISEN, MITIGATING THE INEVITABLE: HOW ORGANIZATIONS MANAGE DATA BREACH EXPOSURES (Mar. 2016), www.advisenltd.com/wp-content/uploads/2016/03/how-organizations-manage-data-breach-exposures-2016-03-03.pdf.
139. *See id.*
140. *See, e.g.*, W. Heritage Ins. Co. v. Asphalt Wizards, 795 F.3d 832 (8th Cir. 2015) (deductible amount not met for TCPA violations due to $1000 per claim deductible); First Mercury Ins. Co. v. Nationswide Sec. Servs., 54 N.E.3d 323 (Ill. App. Ct. 2016) (applying a "per claim" deductible of $500 relating to TCPA damages).
141. *See, e.g.*, CNA Commercial Property Policy Form G-145707-C (2012).

Depending on the policy form, there may be arguments as to whether the insured is entitled to collect under multiple sublimits or whether the entirety of the insured's losses are capped by one of the sublimits in question.[142] Similar issues may arise when the policy contains multiple potentially applicable deductibles.[143] When negotiating a cyber policy, it is important that the policy make clear how multiple sublimits and deductibles will apply in such situations. Where a policy has sublimits, it is also important to review excess policies to be sure they attach in excess of the sublimits as well as applicable aggregates.

[E] Notice Requirements

As noted above, cyber policies are often claims-made policies.[144] But unlike many claims-made policies, particularly in the liability context, cyber polices sometimes require notice to insurers of known occurrences and lawsuits "as soon as practicable" or even "immediately." These clauses are particularly common where insurers are obligated to defend a claim, their theory being that they want to know of the claim as early as possible in order to defend.

Putting aside issues of how soon is practicable or immediate,[145] a question that commonly arises in situations where notice is required

---

142. *See, e.g.*, Hewlett-Packard Co. v. Factory Mut. Ins. Co., 2007 WL 983990 (S.D.N.Y. 2007) (holding that the insured was entitled to collect for property damage up to $50 million under its "electronic data processing" sublimit, as well as its additional losses for business interruption, which were not capped by the electronic data processing sublimit); *see also* Penford Corp. v. Nat'l Union Fire Ins. Co. of Pittsburg, 2010 WL 300838 (N.D. Iowa Jan. 19, 2010) (where the sublimits themselves did not indicate the scope of coverage, court looked to other provisions and allowed extrinsic evidence for clarification).

143. *See, e.g.*, Gen. Star Indem. v. W. Fla. Vill. Inn, 874 So. 2d 26 (Fla. Dist. Ct. App. 2004) (involving the issue of which deductible applied on a policy containing two different deductibles for different types of causes of loss).

144. *See* section 16:3.1[B], *supra*.

145. *See* 8f-198 APPLEMAN ON INSURANCE § 4734 (2013) (what is immediate or practicable depends upon the facts of a particular case and does do not require instantaneous notice); *see also* ALLAN D. WINDT, INSURANCE CLAIMS AND DISPUTES § 1:1 (2010) (the soon-as-practicable standard generally involves a consideration of what is reasonable given the circumstances). Many jurisdictions require the insurer to show prejudice to support a late notice defense. *See, e.g.*, Ins. Co. of Pa. v. Associated Int'l Ins. Co., 922 F.2d 516, 526 (9th Cir. 1990) ("Under California law, the insurer has the burden of proving actual and substantial prejudice."); Nat'l Sur. Corp. v. Immunex Corp., 297 P.3d 688, 696 (Wash. 2013) (same). However, policies requiring notice within the policy period or an extended reporting period are often enforced. *See, e.g.*, James & Hackworth v. Cont'l Cas. Co., 522 F. Supp. 785 (N.D. Ala. 1980) (enforcing provision that required insured to provide notice during the policy period or within sixty days after its expiration).

is when the obligation to give notice is triggered. For many years, practitioners have advised large corporate insureds to limit the obligation to give notice to situations where a specified individual or group of individuals—commonly the risk manager, CFO, or general counsel—has knowledge of the claim. This is especially important in far-flung organizations where an individual who receives knowledge of a claim or potential claim may not be in a position to give notice or even understand that notice is required. Where policies contain these kinds of provisions, courts have repeatedly held them to be enforceable.[146]

The issue of whose knowledge triggers the obligation to give notice takes on particular significance in the context of cyber risks. There may sometimes be a considerable lapse between the time of a covered event and the time when knowledge of that event surfaces. In some cases, knowledge of the event may be confined to front-line information technology personnel who are focused on containing the problem and have no familiarity with insurance or its requirements. As a result, it is important to attempt to negotiate provisions in cyber policies that predicate the requirement to give notice on knowledge by the risk manager, CFO or CIO, or similarly appropriate individuals. It may also be important to develop internal procedures to ensure that insurable claims are brought to the attention of such individuals.

[F] Coverage for Regulatory Investigations or Actions

A major issue in evaluating cyber coverages is the extent to which there is coverage for regulatory investigations or actions. As an example, the Federal Trade Commission (FTC) regularly launches investigations, both formal and informal, into company practices that may violate section 5 of the Federal Trade Commission Act ("FTC Act") by unfairly handling consumer information.[147] Other

---

146. *See, e.g.*, Hudson Ins. Co. v. Oppenheim, 81 A.D.3d 427, 428 (N.Y. App. Div. 2011) (upholding a provision stating: "The subject policy required the insured to provide notice of a loss 'At the earliest practicable moment after discovery of loss by the Corporate Risk Manager,' and provided that 'Discovery occurs when the Corporate Risk Manager first becomes aware of facts.'"); QBE Ins. Corp. v. D. Gangi Contracting Corp., 888 N.Y.S.2d 474, 475 (App. Div. 2009) (enforcing an insurance policy stating: "Knowledge . . . by Your agent, servant or employee shall not in itself constitute knowledge of you unless the Corporate Risk Manager of Your corporation shall have received notice of such Occurrence.").

147. The FTC's power was recently affirmed in FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015), where the federal court rejected a challenge to the FTC's authority to use its section 5 authority to sue merchants for data breaches. After Wyndham suffered several data breaches between 2008 and 2010, the FTC filed an action alleging that Wyndham engaged in unfair practices and that its privacy policy was

regulatory bodies have entered the fray as well. For instance, one Securities & Exchange Commission (SEC) commissioner has stated that even though a company's management team may have primary responsibility for overseeing cyber risk management, the board of directors is responsible for overseeing the implementation and appropriateness of these programs.[148] Cybersecurity cases have become a principal enforcement focus for the SEC, specifically relating to internal controls to protect market integrity and disclosure of material cyber events.[149] Likewise, the Financial Industry Regulatory authority (FINRA) has stated that cybersecurity is an enforcement priority.[150] State attorneys general also exercise investigative and prosecutorial powers in the cyber area, as do regulatory and law enforcement authorities around the globe.[151]

In many instances, coverage for these kinds of situations will turn on the definition of "claim" in the relevant policy.[152] If, for example, a claim is defined as an action for civil damages, regulatory actions may not fall within that category.[153] Most policies address this issue by including a much broader definition of "claim" that encompasses criminal proceedings, claims for injunctive relief, and certain administrative or regulatory proceedings as well.[154]

---

deceptive. *Id*. at 240; *see also* Complaint, *In re* Snapchat, Inc., No. 132 3078 (FTC Dec. 23, 2014) (alleging that Snapchat violated section 5 of the FTC Act by, among other things, falsely representing that its users' messages would permanently disappear and by collecting users' location information); Complaint, *In re* LabMD, Inc., No. 102 3099 (FTC Aug. 28, 2013) (alleging that LabMD violated section 5 of the FTC Act by failing to "provide reasonable and appropriate security for personal information on its computer networks").

148. Comm'r Luis A. Aguilar, Address at Cyber Risks and the Boardroom Conference: Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening Focus (June 10, 2014).

149. *Id*.

150. *See* FINRA, *Report on Cybersecurity Practices*, Feb. 2015, www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf.

151. *See, e.g.*, Press Release, European Union Agency for Network & Info. Sec., *New Regulation for EU Cybersecurity Agency ENISA, with New Duties* (June 18, 2013), www.enisa.europa.eu/news/enisa-news/new-regulation-for-eu-cybersecurity-agency-enisa-with-new-duties.

152. *See also infra* note 214 (discussing exclusion for failure to consistently implement cyber risk controls).

153. *See, e.g.*, Passaic Valley Sewerage Comm'rs v. St. Paul Fire & Marine Ins. Co., 21 A.3d 1151, 1159 (N.J. 2011) (rejecting an insured's coverage for a claim for injunctive regulatory relief because, under the policy, a claim was defined as one for civil damages).

154. *See, e.g.*, CHUBB Forefront for Insurance Companies Form 17-02-17 (1999) ("Claim means: (i) a written demand for monetary damages or non-monetary relief; (ii) a civil proceeding commenced by the service of a

As illustrated by various cases involving D&O liability policies, the definition of claim can be very important in establishing the degree of formality required for coverage to be available for a particular regulatory initiative. Some policies, for example, require the filing of a notice of charges, an investigative order, or similar document. Under such policies, insurers may attempt to require a proceeding initiated by formal administrative action as a precondition to coverage. This can be problematic since many administrative initiatives are informal and, in many cases, policyholders would prefer that they remain at an informal stage.

The issue is illustrated by cases like *Office Depot, Inc. v. National Union Fire Insurance Co. of Pittsburgh, Pa.*[155] and *MBIA, Inc. v. Fed. Ins. Co.*[156] In the *Office Depot* case, the policyholder sought coverage for an SEC investigation into assertions it had selectively disclosed certain non-public information in violation of federal securities laws.[157] While the SEC's investigation of Office Depot had commenced in 2007, no subpoena was issued until 2008.[158] The policy contained coverage for a "securities claim," but the definition of "securities claim" specifically carved out "an administrative or regulatory proceeding against, or investigation of the [company]" unless "during the time such proceeding is also commenced and continuously maintained against an Insured Person."[159] Recognizing that the policy

---

complaint or similar pleading; (iii) a criminal proceeding commenced by the return of an indictment; or (iv) a formal administrative or regulatory proceeding."); Liberty Mutual Group: Liberty Insurance Underwriters, Inc. General D&O Form US/D&O2000-POL (Ed. 1/00) (2004) ("The definition of claim includes a written demand for monetary or nonmonetary relief, a civil or criminal proceeding or arbitration, a formal administrative or regulatory proceeding, or a formal criminal, administrative investigation commenced.").

155. Office Depot, Inc. v. Nat'l Union Fire Ins. Co., 453 F. App'x 871 (11th Cir. 2011).

156. MBIA, Inc. v. Fed. Ins. Co., 652 F.3d 152 (2d Cir. 2011).

157. *Office Depot*, 453 F. App'x at 871.

158. *Id.* at 874.

159. As the court explained:

> Two policy provision[s] are relevant to the disposition of this issue. First, the insuring agreement language provides:
>
> > COVERAGE B: ORGANIZATION INSURANCE
> >
> > (i) *Organization Liability*. This policy shall pay the Loss of any Organization arising from a Securities Claim made against such Organization for any Wrongful Act of such Organization. . . .
>
> The policy defines a Securities Claim as:
>
> > a Claim, *other than an administrative or regulatory proceeding against, or investigation of an Organization*, made against any Insured:

provided coverage for regulatory or administrative proceedings under certain circumstances, the Eleventh Circuit held that the policy did not provide coverage for administrative or regulatory "investigations."[160] The *Office Depot* court held that informal requests by the SEC were part of an investigation that did not become a proceeding and subject to coverage until the issuance of a subpoena.[161]

A different approach is illustrated by the *MBIA* case. There, the policyholder, MBIA, sought coverage for an SEC investigation into its reporting of three financial transactions.[162] While the SEC obtained a formal investigatory order, it did not issue subpoenas to MBIA because MBIA had asked the SEC to "accept voluntary compliance with their demands for records in lieu of subpoenas to avoid adverse publicity for MBIA."[163] The policy provided coverage for any "formal or informal administrative or regulatory proceeding or inquiry commenced by the filing of a notice of charges, formal or informal investigative order or similar document."[164] The insurers argued that because the SEC's investigation of MBIA had proceeded through oral requests, as opposed to subpoenas or other formal processes, the SEC investigation was not covered under the policy.[165] The Second Circuit held that the oral requests were issued pursuant to a formal investigative order and thus constituted securities claims under the policy.[166] The Second Circuit went on to state that "insurers cannot require that as an investigation proceeds, a company must suffer extra public relations damage to avail itself of coverage a reasonable person would think was triggered by the initial investigation."[167]

---

(1) alleging a violation of any federal, state, local or foreign regulation, rule or statute regulating securities . . . ; or

(2) brought derivatively on the behalf of an Organization by a security holder of such Organization.

Notwithstanding the foregoing, the term "Securities Claim" *shall include an administrative or regulatory proceeding* against an Organization, but only if and only during the time such proceeding is also commenced and continuously maintained against an Insured Person.

Id. at 875.

160. *Id.* at 877.
161. *Id.* at 878.
162. *MBIA*, 652 F.3d at 160.
163. *Id.* at 156.
164. *Id.* at 159.
165. *Id.* at 161.
166. *Id.* at 162.
167. *Id.* at 161.

Modern policies, including cyber policies, have dealt with these issues in a variety of ways, including provisions providing explicit coverage for informal inquiries or the cost of preparing an individual to testify, but some of these provisions do not cover the substantial cost that the company, as opposed to the individual, may be forced to incur, particularly where there is extensive electronic discovery or document productions. Insureds generally should seek coverage with a low threshold for what triggers coverage in relation to a regulatory investigation.

Another issue that is sometimes raised by insurers where policyholders seek coverage for a regulatory investigation or action is whether there has been a "Wrongful Act" under the definitions in the relevant policy. For example, in *Employers' Fire Ins. Co. v. ProMedica Health Sys., Inc.*,[168] the court considered whether there was coverage for a FTC antitrust investigation[169] that culminated in the FTC initiating an administrative proceeding against the policyholder.[170] The policy in *ProMedica* defined "Wrongful Act" to include "'any actual or alleged' antitrust violation."[171] Rejecting several contrary decisions, the *ProMedica* court concluded that the FTC investigation was not "for a Wrongful Act" because the FTC did not "affirmatively accuse [the policyholder] of antitrust violations" until it filed its January 13, 2011 administrative action.[172] According to the court, until the commencement of an administrative action, the FTC investigation had merely sought to determine *whether* the policyholder had committed antitrust violations.[173] Thus, the *ProMedica* court held that there was no coverage under the policy until August 2011 when the FTC filed a complaint against the policyholder alleging various antitrust violations.[174]

The requirement of a "Wrongful Act" was also recently confronted in one of the few reported decisions interpreting a cyber risk policy.[175] In *Federal Recovery Services*, the court held that the insurer had no duty to defend its insured under its CyberFirst policy in a suit where

---

168. Emp'rs Fire Ins. Co. v. ProMedica Health Sys., Inc., 524 F. App'x 241 (6th Cir. 2013).
169. Note that the insurer in *ProMedica* had denied coverage on the basis that the policyholder's notice was not timely; thus, it was the policyholder, not the insurer, arguing that a "Claim" had not arisen under the policy until the filing of the Federal Trade Commission's administrative proceedings.
170. *Emp'rs Fire Ins.*, 524 F. App'x at 243.
171. *Id*. at 247.
172. *Id*. at 248.
173. *Id*. at 250.
174. *Id*. at 251.
175. Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., 103 F. Supp. 3d 1297 (D. Utah 2015).

the sole allegations related to intentional conduct—that the insured refused to return its client's customer information.[176] The court reasoned that the claims were not an "error, omission, or negligent act" as required by the policy since the underlying lawsuit alleged that the insured acted willfully and with malice.[177]

Many cyber policies eliminate these issues by not including the same kind of requirements for "formal investigation" or specific assertions of "Wrongful Acts" that sometimes exist in other types of traditional policies. The extent of coverage for regulatory investigations and informal actions, as well as coverage for regulatory remedies and the availability of defense coverage,[178] should be carefully considered in evaluating cyber coverage.

[G] Definition of Loss

Another area raised by regulatory activities is coverage for fines, penalties, and disgorgement. Some policies purport to exclude coverage for fines and penalties or for violations of law.[179] Others explicitly provide such coverage.[180]

Even where such remedies are covered by the policy language, insurers sometimes argue that the coverage is contrary to public policy. This issue was considered by the Illinois Supreme Court in *Standard Mutual Insurance Co. v. Lay*,[181] where the insurer argued that statutory damages of $500 per violation under the Telephone Consumer Protection Act[182] should be denied as akin to punitive damages. Some states hold that coverage for punitive damages is contrary to public

---

176. *Id*. at 1302.
177. *Id*.
178. *See* notes 191 and 193, *infra*, and accompanying text.
179. *See, e.g.*, Mortenson v. Nat'l Union Fire Ins. Co., 249 F.3d 667, 669 (7th Cir. 2001) ("the policy excludes losses consisting of 'fines or penalties imposed by law or other matters'"); Hartford Fire Ins. Co. v. Guide Corp., 2005 WL 5899840, at *2 (S.D. Ind. Feb. 14, 2005) (policy at issue "contains an exclusion for punitive damages, fines, and penalties"); *see also* Big 5 Sporting Goods Corp. v. Zurich Am. Ins. Co., 957 F. Supp. 2d 1135 (C.D. Cal. 2013) (adopting insurer argument that civil penalties, attorney fees, and disgorgement under California statute are not covered damages under insurance policy), *aff'd*, 635 F. App'x 351 (9th Cir. 2015); notes 86–87, *supra*.
180. *See, e.g.*, Taylor v. Lloyd's Underwriters of London, 1994 WL 118303, at *7 (E.D. La. Mar. 25, 1994) (contract stated: "Clause (9) of the P&I policy actually *extends* coverage for: Liability for fines and penalties. . . .") (emphasis in original); CNA Insurance Company, Fiduciary Liability Solutions Policy, GL2131XX (2005) (insurance policy covered a percentage of liability for fines and penalties for violations of ERISA, its English equivalent, and HIPAA requirements).
181. Standard Mut. Ins. Co. v. Lay, 989 N.E.2d 591 (Ill. 2013).
182. *See* note 77, *supra*.

policy[183] or is allowed only under limited circumstances.[184] After a careful analysis of the history of the statute, the Illinois Supreme Court concluded in *Lay* that the statutory damages under the TCPA were compensatory in nature and not precluded by public policy.[185] In an effort to avoid such issues, many policies contain provisions that allow coverage for punitive damages or regulatory remedies to be governed by "favorable law" or by law of a specific jurisdiction such as England or Bermuda, which have case law permitting such coverage.[186]

There also has been active litigation in recent years concerning the availability of insurance for certain regulatory remedies such as disgorgement. In some cases, the issue is dealt with as an issue of public policy with different courts taking different views of the issue. While some cases suggest that disgorgement of ill-gotten gains may not be insurable as a matter of public policy,[187] others come to a

---

183. *See, e.g.*, Ace Am. Ins. Co. v. Dish Network LLC, 2016 WL 1182744 (D. Colo. Mar. 28, 2016) (holding that an award of $500 per TCPA violation "constitutes a penalty or an ilk of punitive damages which may not be covered by insurance"); Soto v. State Farm Ins. Co., 635 N.E.2d 1222, 1224 (N.Y. 1994) ("a rule permitting recovery for excess civil judgments attributable to punitive damage awards would be unsound public policy").

184. *See, e.g.*, Magnum Foods, Inc. v. Cont'l Cas. Co., 36 F.3d 1491, 1497–98 (10th Cir. 1994) (holding that insurance coverage of punitive damages is against public policy, except when the party seeking coverage has been held liable for punitive damages solely under vicarious liability) (internal citation omitted).

185. *Lay*, 989 N.E.2d at 599–602; *see also* Evanston Ins. Co. v. Gene by Gene Ltd., 155 F. Supp. 3d 706 (S.D. Tex. 2016) (holding that the request for actual and statutory damages "falls under the Policies' definition of damages"); Columbia Cas. Co. v. HIAR Holding, LLC, 411 S.W.3d 258 (Mo. 2013) (holding that "TCPA statutory damages of $500 per occurrence are not damages in the nature of fines or penalties").

186. *See, e.g.*, Lancashire Cty. Council v Mun. Mut. Ins. Ltd [1997] QB 897 (Eng.) ("There is no present authority in English law which establishes that it is contrary to public policy for an insured to recover under a contract of insurance in respect of an award of exemplary damages whether imposed in relation to his own conduct or in relation to conduct for which he is merely vicariously liable. Indeed newspapers, we are told, regularly insure against exemplary damages for defamation.").

187. *See, e.g.*, Ryerson Inc. v. Fed. Ins. Co., 676 F.3d 610, 613 (7th Cir. 2012) (describing a policy that covers disgorgement of ill-gotten gains and stating that "no state would enforce such an insurance policy"); Unified W. Grocers, Inc. v. Twin City Fire Ins. Co., 457 F.3d 1106, 1115 (9th Cir. 2006) ("California case law precludes indemnification and reimbursement of claims that seek the restitution of an ill-gotten gain") (citation omitted); Level 3 Commc'ns, Inc. v. Fed. Ins. Co., 272 F.3d 908, 910 (7th Cir. 2001) (district court should have ruled that disgorging profits of theft is against

different conclusion.[188] In some cases, decisions turn on whether there is a true disgorgement of profits, the regulator is a pass-through, or a disgorgement is a surrogate measure of damages.[189]

Putting public policy arguments aside, the language of the policy may be important. It is more difficult for insurers to argue that disgorgement is not covered where the policy covers "loss" as opposed to "damages."[190] Depending on policy wording, defense costs may be covered with respect to a disgorgement claim even where a court holds that public policy precludes indemnity coverage.[191] Similarly, an insurer may be obligated to pay defense costs though a regulatory remedy may not be covered, as long as the regulatory proceeding

---

public policy); Mortenson v. Nat'l Union Fire Ins. Co., 249 F.3d 667, 672 (7th Cir. 2001) ("It is strongly arguable, indeed, that insurance against the section 6672(a) penalty, by encouraging the nonpayment of payroll taxes, is against public policy[.]").

188. *See, e.g.*, Genzyme Corp. v. Fed. Ins. Co., 622 F.3d 62, 69 (1st Cir. 2010) ("We see no basis in Massachusetts legislation or precedent for concluding that the settlement payment is uninsurable as a matter of public policy."); Westport Ins. Corp. v. Hanft & Knight, P.C., 523 F. Supp. 2d 444, 453 (M.D. Pa. 2007) (finding an insurer's argument that public policy prohibits coverage for disgorgement "unavailing"); Genesis Ins. Co. v. Crowley, 495 F. Supp. 2d 1110, 1120 (D. Colo. 2007) (court declined to adopt insurer's argument that disgorgement is uninsurable as a matter of public policy); BLaST Intermediate Unit 17 v. CNA Ins. Cos., 674 A.2d 687, 689–90 (Pa. 1996) (finding that coverage for disgorgement of ill-gotten gains did not violate public policy).

189. *See, e.g.*, JP Morgan Sec., Inc. v. Vigilant Ins. Co., 992 N.E.2d 1076 (N.Y. 2013) (denying motion to dismiss filed by insurers on the ground that payment by Bear Stearns constituted uninsurable disgorgement where Bear Stearns agreed to pay $160 million designated as "disgorgement" in the SEC order but "the SEC order does not establish that the $160 million disgorgement payment was predicated on moneys that Bear Stearns itself improperly earned as a result of its securities violations"); Limelight Prods., Inc. v. Limelite Studios, Inc., 60 F.3d 767, 769 (11th Cir. 1995) ("recognizes ill-gotten profits as merely another form of damages that the statute permits to be presumed because of the proof unavailability in these actions").

190. *Compare* Chubb Custom Ins. Co. v. Grange Mut. Cas. Co., 2011 U.S. Dist. LEXIS 111583, at *31 (S.D. Ohio Sept. 29, 2011) (a policy's definition of loss covered wrongfully retained money), *with* Cont'l Cas. Co. v. Duckson, 826 F. Supp. 2d 1086, 1097 (N.D. Ill. 2011) ("return of profits obtained illegally does not constitute covered damages").

191. *See, e.g.*, Vigilant Ins. Co. v. Credit Suisse First Bos. Corp., 2003 WL 24009803, at *5 (N.Y. Sup. Ct. July 8, 2003) (finding that because the "term 'loss' includes defense costs," insurer must pay for them, even though the remedy for disgorgement of ill-gotten gains is not insurable as a matter of public policy).

constitutes a claim under the applicable policy definition.[192] Finally, as noted above, policies sometimes contain specific choice-of-law provisions requiring application of the law of a jurisdiction that favors coverage for remedies like fines or penalties.[193]

[H] Who Controls Defense and Settlement

The issue of who controls the selection of counsel, the course of defense, and decisions whether to settle can be extremely important under any insurance policy. Many policies, including cyber policies, give the insurer varying degrees of control over these issues. An insured should carefully consider these matters at the time a policy is being negotiated, when there may be some flexibility on both sides, as opposed to after a claim arises.

With respect to the selection of counsel, many insurance policies that contain the duty to defend give the insurance company the unilateral right to appoint counsel unless there is a reservation of rights or some other situation that gives the insured the right to appoint counsel at the insurer's expense.[194] Policyholders are often surprised to find that they are confronted with a case that is very important to them but that their policy allows the attorneys or other professionals to be selected and controlled in varying degrees by the insurer. While this may be appropriate in routine matters without significant reputational or other exposure to the company, or in situations where there is a service that has been bargained and paid for by the insured, many insureds confronted with a cyber breach prefer to select and utilize their own counsel. It is important that policy language be negotiated that permits this approach if that is what is desired.

---

192. *See, e.g.*, Bodell v. Walbrook Ins. Co., 119 F.3d 1411, 1414 (9th Cir. 1997) (holding that an insurer must pay defense costs related to a U.S. Postal Inspection Service investigation, as the regulatory proceeding constituted a claim under the policy, even though a remedy for fraud would not be covered).

193. *See* text accompanying *supra* note 185.

194. *Compare* Twin City Fire Ins. Co. v. Ben Arnold-Sunbelt Beverage Co., 433 F.3d 365, 366 (4th Cir. 2005) ("The insurance company, in turn, typically chooses, retains, and pays private counsel to represent the insured as to all claims."), *with* HK Sys., Inc. v. Admiral Ins. Co., 2005 WL 1563340, at *16 (E.D. Wis. June 27, 2005) (when there is a conflict of interest between the insurer and the insured, "the insurer retains the right either to choose independent counsel or to allow the insured to choose counsel at the insurer's expense"), San Diego Navy Fed. Credit Union v. Cumis Ins. Soc'y, 208 Cal. Rptr. 494, 506 (Ct. App. 1984) ("[T]he insurer must pay the reasonable cost for hiring independent counsel by the insured . . . [and] may not compel the insured to surrender control of the litigation."), *superseded by* CAL. CIV. CODE § 2860 (2012), *and* Md. Cas. Co. v. Peppers, 355 N.E.2d 24, 31 (Ill. 1976) (insured "has the right to be defended . . . in case by an attorney of his own choice" that is paid for by insurer, when there is a conflict between insurer and insured).

A compromise position in some policy forms involves the use of "panel counsel." Under this approach, the policyholder is entitled to select counsel for the defense of the claim, but choices are restricted to a list of lawyers designated by the insurer. In some cases, the list is appended to the policy. In others, it is set forth on a website maintained by the insurer.[195] In either case, at least in the absence of a conflict, the policyholder may be contractually limited to selecting counsel from the panel counsel list.

The panel counsel lists of most major insurance companies include some well-known and able lawyers; however, there can be problems with the panel counsel approach from the insured's prospective. First, panel counsel often expect to receive an ongoing flow and volume of work from the insurance company. As a result, they may be extremely attentive to the insurance company's approach and the way in which it wants to handle cases. Second, in some cases, panel counsel have agreed to handle cases for a particular insurance company's insureds at sharply discounted rates. In some cases, these rate requirements may preclude from the panel firms with major expertise in a particular area. In others, they may incentivize insurers to use less experienced lawyers. Third, panel counsel are not necessarily lawyers typically used by the policyholder. As a result, they may have no familiarity with the policyholder or its business and management and may lack the trust built by a long attorney-client relationship.

In light of these concerns, it is important to review carefully any panel counsel provisions in a particular policy. In many cases where a company has a "go-to" counsel that it expects to use in the event of a covered claim, the insurance company will agree in advance to include those lawyers on their panel counsel list for that particular insured. This is an issue that should be considered when the policy is being negotiated since it is frequently easier to negotiate inclusion of a policyholder's normal counsel at the time the policy is being negotiated, as opposed to after a claim has occurred.

The issue of selection of counsel is closely aligned to the questions of control of defense and control of settlement. Particularly where there is a duty to defend, the insurer may have a high degree of control of the defense of a claim. While disagreements between the insurer and the insured on defense strategy may raise difficult issues,[196] the key for present purposes is, again, to consider the matter when the policy

---

195. *See, e.g.*, Panel Counsel Directory, AIG (May 24, 2013), www-238.aig.com/default.aspx; *Approved Panel Counsel Defense Firms*, CHUBB GROUP OF INSURANCE COMPANIES (July 5, 2012, 3:30 PM), www.chubb.com/businesses/csi/chubb8548.html.

196. *See, e.g.*, N. Cty. Mut. Ins. Co. v. Davalos, 140 S.W.3d 685, 689 (Tex. 2004) ("Every disagreement [between insurer and insured] about how the defense should be conducted cannot amount to a conflict of interest. . . . If

is being negotiated so the insured understands the implications of the policy being purchased. At a minimum, the insured will almost always have a duty to cooperate with its insurer that raises issues about privilege and other matters.[197] In addition, policies may include insurer rights to consent to covered expenditures that should be reviewed both when a policy is negotiated and in the event of a claim.[198]

These issues may be particularly significant in the area of settlement. Most policies give an insurer the right to consent to any settlement. In some cases, a policyholder may want to settle and the insurer believes the amount proposed is excessive. In certain circumstances, the insurer can refuse to consent,[199] but may face liability in

---

it did, the insured, not the insurer, could control the defense by merely disagreeing with the insurer's proposed actions."). *See generally* 3 JEFFREY E. THOMAS, NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 17.07 (2012).

197. *See, e.g.*, Martinez v. Infinity Ins. Co., 714 F. Supp. 2d 1057 (C.D. Cal. 2010) (insurance policy at issue imposed upon the insured a duty to cooperate to hand over privileged financial documents, car payment records, and maintenance records to the insurer); Kimberly-Clark Corp. v. Cont'l Cas. Co., 2006 U.S. Dist. LEXIS 63576, at *5 (N.D. Tex. Aug. 18, 2006) ("attorney-client communications or attorney work product . . . are not abrogated by the cooperation clause"); Purze v. Am. Alliance Ins. Co., 781 F. Supp. 1289, 1292–93 (N.D. Ill. 1991) (the duty to cooperate in the insurance contract at issue involved insured giving insurer banking information); Remington Arms Co. v. Liberty Mut. Ins. Co., 142 F.R.D. 408, 416 (D. Del. 1992) (even when an insured has a duty to cooperate with insurer, "insurance coverage actions did not foreclose the assertion of attorney-client privilege"); Waste Mgmt., Inc. v. Int'l Surplus Lines Ins. Co., 579 N.E.2d 322, 327 (Ill. 1991) ("condition in the policy requiring cooperation on the part of the insured is one of great importance. . . . A fair reading of the terms of the contract renders any expectation of attorney-client privilege, under these circumstances, unreasonable."). *See generally* 3 JEFFREY E. THOMAS, NEW APPLEMAN ON INSURANCE LAW LIBRARY EDITION § 16.04 (2012).

198. *See, e.g.*, CHUBB CyberSecurity Form 14-02-14874, § XIV.C (2009) ("No Insured shall settle or offer to settle any Claim . . . without the Company's prior written consent"). *But see* Booking v. Gen. Star Mgmt. Co., 254 F.3d 414, 421 (2d Cir. 2001) ("[A] breach of a 'settlement-without-consent' clause is material only if it prejudices the insurer.") (internal citation omitted) (applying Texas law); Progressive Direct Ins. Co. v. Jungkans, 972 N.E.2d 807, 811 (Ill. App. Ct. 2012) ("[A]n insurer who invokes a cooperation clause must affirmatively show that it was prejudiced by the insured's failure to notify it in advance of his settlement with the tortfeasor.").

199. *See, e.g.*, Certain Underwriters of Lloyd's v. Gen. Accident Ins. Co. of Am., 909 F.2d 228, 232 (7th Cir. 1990) (an insurer may refuse to settle, as "the insurer has full control over defense of the claim, including the decision to settle").

excess of policy limits if the insured is later required to pay a judgment in excess of the proposed settlement.[200]

Alternatively, the insurer may want to settle where the policyholder does not. Some policies give the insurer the right to do this, while other policies and case law do not.[201] Some policies provide that where an insurer wants to settle and an insured does not, only a portion of fees and settlement costs will be covered in the future.[202] Again, the starting place is the policy, so the language should be considered at the time the policy is negotiated.

[I] Control of Public Relations Professionals

Many cyber policies provide coverage for certain kinds of crisis management activities, which may encompass expenses of public relations experts and certain kinds of advertising.[203] Typically, the dollar limits for such coverages are relatively low, but these coverage provisions may cede control of public relations experts and budget, in varying degrees, to the insurer. Media experts who deal with cyber privacy breaches can have special expertise, and some policyholders

---

200. *See, e.g.*, Nat'l Union Fire Ins. Co. v. Cont'l Ill. Corp., 673 F. Supp. 267, 270 (N.D. Ill. 1987) ("Illinois has long recognized an insured's right to hold the insurer responsible for an amount in excess of the policy limits when the insurer has been guilty of fraud, bad faith or negligence in refusing to settle the underlying claim against the insured within those limits."); Am. Hardware Mut. Ins. Co. v. Harley Davidson of Trenton, Inc., 124 F. App'x 107, 112 (3d Cir. 2005) ("The *Rova Farms* rule is thus: (1) if a jury could find liability, (2) where the verdict could exceed the policy limit, and (3) the third-party claimant is willing to settle within the policy limit, then (4) in order to be deemed to have acted in good faith, the insurer must initiate settlement negotiations and exhibit good faith in those negotiations. American Hardware was obligated to initiate settlement negotiations and did not; therefore it acted in bad faith and is liable for the excess verdict.").

201. *Compare* Sec. Ins. Co. v. Schipporeit, Inc., 69 F.3d 1377, 1383 (7th Cir. 1995) (policy required the insured's consent to a settlement), *and* Brion v. Vigilant Ins. Co., 651 S.W.2d 183, 184 (Mo. Ct. App. 1983) (terms of the policy required the insured's consent), *with* Papudesu v. Med. Malpractice Joint Underwriting Ass'n of R.I., 18 A.3d 495, 498–99 (R.I. 2011) (insurance policy gave the insurer the right to settle "as it deems expedient," even without insured's consent).

202. *See, e.g.*, CHUBB CyberSecurity Form 14-02-14874, § XIV.D (2009) ("If any Insured withholds consent to any settlement acceptable to the claimant . . . then the Company's liability for all Loss, including Defense Costs, from such Claim shall not exceed the amount of the Proposed Settlement plus Defense Costs incurred[.]").

203. *See, e.g.*, CHUBB CyberSecurity Form 14-02-14874, § I.C. (2009) (providing coverage for crisis management expenses, which includes advertising and public relations media and activities).

view insurer expertise in selecting the right experts and managing these kinds of situations as one of the benefits of purchasing coverage. Other policyholders may not wish to relinquish control of these issues, particularly where limits applicable to crisis management expenses are small. In some cases, the policyholder may deal with these issues by negotiating with the insurer to include the policyholder's chosen expert as an option under the policy. In any event, selection and management of public relations professionals, like selection of defense attorneys, is an issue that should be evaluated in purchasing cyber coverages.

[J] Issues Created by Policyholder Employees

Some policies exclude "loss caused by an employee."[204] This kind of exclusion can be problematic in a cyber policy where cyber issues may sometimes involve an inside job.

Even where there is not a blanket employee exclusion, insurance policies often preclude coverage for liabilities expected or intended or damage knowingly caused by "the insured."[205] A common question in insurance contracts, which is equally significant in the context of cyber policies, is whose knowledge controls the applicability of potentially applicable exclusions.

The obvious concern in the cyber context is the situation where an employee is intentionally responsible for a privacy breach or perhaps for selling confidential information to others. Resultant claims against the employee are likely excluded, in varying degrees, by most insurance policies. But the question that arises is whether any applicable exclusions are limited to the responsible employee or the corporate policyholder as a whole.

Case law developed under traditional insurance coverages has varied with respect to the extent to which knowledge or intentional misconduct by an employee can be attributed to the policyholder for purposes of denying coverage. Some cases require the knowledge to be

---

204. *See, e.g.*, Ace American Insurance Company Commercial Crime Policy, www.acegroup.com/us-en/assets/commercial-crime-policy-loss-sustained-form.pdf (last visited Sept. 27, 2016).

205. *See, e.g.*, Everest Nat'l Ins. Co. v. Valley Flooring Specialties, 2009 U.S. Dist. LEXIS 36757, at *19 (E.D. Cal. Apr. 14, 2009) ("intentional and knowing conduct exclusions unambiguously apply"); Auto Club Grp. Ins. Co. v. Marzonie, 527 N.W.2d 760, 768 (Mich. 1994) (policy precluded coverage for injury that was intended or activity that "the actor knew or should have known" would cause injury), *abrogated by* Frankenmuth Mut. Ins. Co. v. Masters, 595 N.W.2d 832 (Mich. 1999). *See generally* 3 ALLAN WINDT, INSURANCE CLAIMS AND DISPUTES § 11:9 (6th ed. 2013).

by a senior person or officer or director for the intent to be attributed to the company.[206] Others may not.[207]

Today, many policies deal with this issue by a severability clause. A typical such clause states that no fact pertaining to and no knowledge possessed by any insured person shall be imputed to another insured person, and many specify that only the knowledge of certain company officers is imputed to the company.[208] Under such clauses, the knowledge or intent is limited to the relevant individual and not attributed to others.[209]

A second issue with these kinds of exclusions concerns the situation where knowledge or intent is disputed. While some policies limit the ability of an insurer to deny coverage in this context to situations in which there has been a "final adjudication," the courts vary on whether such adjudication must be in an underlying case or can be in an insurance coverage case, including one initiated by the carrier.[210]

---

206. *See, e.g.*, Legg Mason Wood Walker, Inc. v. Ins. Co. of N. Am., 1980 U.S. Dist. LEXIS 13088, at *18 (D.D.C. July 24, 1980) (because neither of individuals involved in intentional misconduct was an officer, director, stockholder, or partner, the insured's claim is still covered by insured).

207. *See, e.g.*, FMC Corp. v. Plaisted & Cos., 72 Cal. Rptr. 2d 467, 61 Cal. App. 4th 1132, 1212–13 (Ct. App. 1998) (upholding jury instructions that stated "[K]nowledge which a corporation's employee receives or has in mind when acting in the course of his or her employment is in law the knowledge of the corporation, if such knowledge concerns a matter within the scope of the employee's duties"), *overruled by* California v. Cont'l Ins. Co., 281 P.3d 1000 (Cal. 2012).

208. *See, e.g.*, CHUBB CyberSecurity Form 14-02-14874, § IV (2009) ("for the purposes of determining the applicability of [certain exclusions] . . . A. no fact pertaining to or knowledge possessed by any Insured Person shall be imputed to any other Insured Person to determine if coverage is available; and B. only facts pertaining to or knowledge possessed by an Insured Organization's [certain executive officers] shall be imputed to such Insured Organization to determine if coverage is available"); *see generally* 4 JEFFREY E. THOMAS, APPLEMAN ON INSURANCE § 26.07 (2012).

209. *See, e.g.*, Chrysler Ins. Co. v. Greenspoint Dodge of Houston, Inc., 297 S.W.3d 248, 253 (Tex. 2009) (stating, in the context of a severability clause, "intent and knowledge for purposes of coverage are determined from the standpoint of the particular insured, uninfluenced by the knowledge of any additional insured").

210. *See, e.g.*, Wintermute v. Kan. Bankers Sur. Co., 630 F.3d 1063 (8th Cir. 2011) (insurer not relieved of duty to defend based on personal profit and dishonesty exclusions unless proven in underlying case that the director actually received personal gain or was involved in dishonest acts); Pendergest-Holt v. Certain Underwriters at Lloyd's of London, 600 F.3d 562, 573 (5th Cir. 2010) ("in fact" language is read more broadly than a "final adjudication" clause and satisfied by a final judgment in either the underlying case or a separate coverage case); Atl. Permanent Fed. Sav. & Loan Ass'n v. Am. Cas. Co., 839 F.2d 212 (4th Cir. 1988) (the exclusion does not apply unless there is a judgment adverse to the officers and directors in the underlying suit); *see also infra* notes 211–13.

Many policies deal with this issue in a final adjudication clause. An illustrative policy provision provides:

> The company shall not be liable under Insuring Clause X for Loss on account of any Claim made against any Insured Person:
>
> (a) based upon, arising from, or in consequence of any deliberately fraudulent act or omission or any willful violation of any statute or regulation by such Insured Person, if a *final, non-appealable adjudication in any underlying proceeding or action* establishes such a deliberately fraudulent act or omission or willful violation; or
>
> (b) based upon, arising from, or in consequence of such Insured Person having gained any profit, remuneration or other advantage to which such Insured Person was not legally entitled, if a *final, non-appealable adjudication in any underlying proceeding* or action establishes the gaining of such a profit, remuneration or advantage.[211]

Note that the specific reference to "underlying proceeding" is designed to require the adjudication in the underlying case.[212]

These kinds of provisions are important to policyholders. They are typically construed to require defense and indemnity in the absence of a final adjudication so that the insured is entitled to coverage in the event of a settlement where there has never been an actual adjudication of wrongdoing.[213]

Another type of exclusion involving company employees seeks to preclude coverage for failure to consistently implement cyber risk controls.[214] These kinds of exclusions need to be carefully vetted and limited to specific policies and procedures to avoid subsequent differences as to what is a relevant procedure and what is not.

---

211. *See, e.g.*, Chubb D&O Policy Form 14-02-18489 (2012) (emphasis added).

212. *See generally* Dan A. Bailey, *D&O Policy Commentary, in* INSURANCE COVERAGE 2004: CLAIM TRENDS & LITIGATION, at 205, 215 (PLI Litig. & Admin. Practice, Course Handbook Ser. No. 702, 2004) (when a D&O policy requires "final adjudication" in the underlying action to trigger an exclusion, courts have held that the adjudication must occur in the underlying proceeding and not in a parallel coverage action).

213. *See, e.g.*, Atl. Permanent Fed. Sav. & Loan Ass'n v. Am. Cas. Co., 839 F.2d 212 (4th Cir. 1988) (the exclusion does not apply unless there is a final judgment adverse to the officers and directors in the underlying suit).

214. *See, e.g.*, Complaint, Columbia Cas. Co. v. Cottage Health Sys., No. 15-cv-03432 (C.D. Cal. May 7, 2015) (excluding "[a]ny failure of an Insured to continuously implement the procedures and risk controls identified in the Insured's application . . . and all related information submitted to the Insurer").

[K] Coverage of a *Threatened* Security Breach

Most insurance policies cover actual damages.[215] The common liability policy, for example, covers bodily injury, property damage, and advertising injury. Property damage policies typically cover direct physical damage.[216] While some property damage policies also cover costs to avoid certain harm to physical property,[217] that may not always encompass a security breach, much less a threatened security breach (sometimes referred to as a "ransomware attack"). Cyber policies typically deal with this risk explicitly by covering the cost to respond to a threat of first-party loss or third-party liability due to a cyber breach.[218] It is important to review a cyber policy carefully to be sure that threats, as opposed to only actual damage, are covered,[219] especially in light of the increasing frequency of extortionist cyber threats and ransomware attacks.[220] It is also important to evaluate policy language to determine if the policy only covers threats to extort money or other kinds of threats as well.

---

215. *See, e.g.*, QBE Ins. Corp. v. ADJO Contracting Corp., 934 N.Y.S.2d 36 (Sup. Ct. 2011) ("A policy is implicated when the insured learns of an actual loss or injury covered by the policy, and not when the insured learns only of a potentially dangerous condition.") (citing Chama Holding Corp. v. Generali-US Branch, 22 A.D.3d 443, 444–45 (N.Y. App. Div. 2005)). *But see* Baughman v. U.S. Liab. Ins. Co., 662 F. Supp. 2d 386, 393 (D.N.J. 2009) ("court-ordered medical monitoring with costs to be paid by defendants . . . is 'damages' under [the policy]," even though not actual damage).

216. *See, e.g.*, Wash. Mut. Bank v. Commonwealth Ins. Co., 2006 Wash. App. LEXIS 1316, at *6–7 (Ct. App. June 26, 2006) (holding that plain language of property damage policy required "direct physical loss of or damage to insured property").

217. *Id*. at *11.

218. *See, e.g.*, CHUBB CyberSecurity Form 14-02-14874, § I.J (2009) ("The Company shall pay E-Threat Expenses resulting directly from an Insured having surrendered any funds or property to a natural person who makes a Threat directly to an Insured during the Policy Period."); Philadelphia Insurance Co. Cyber Security Liability Coverage Form PI-CYB-001, § I.C (2010) ("We will reimburse you for the extortion expenses and extortion monies . . . paid by you and resulting directly from any credible threat or series of credible threats.").

219. Some recent case law suggests that increased risk of future harm after a cyber-attack may be sufficient for plaintiffs' standing. *See, e.g.*, *In re* Adobe Sys. Privacy Litig., 66 F. Supp. 3d 1197 (N.D. Cal. 2014).

220. *See, e.g.*, JAMES SCOTT & DREW SPANIEL, INST. FOR CRITICAL INFRASTRUCTURE TECH., THE ICIT RANSOMWARE REPORT 3 (2016) (warning that "2016 is the year ransomware will wreak havoc on America's critical infrastructure community"); Press Release, Fed. Financial Insts. Exam. Council, FFIEC Releases Statement on Cyber Attacks Involving Extortion (Nov. 3, 2015) (notifying members of "the increasing frequency and severity of cyber attacks involving extortion"), www.ffiec.gov/press/pr110315.htm.

[L] Governmental Activity Exclusion

Cyber policies should also be reviewed for provisions limiting coverage for government-sponsored activities. Traditional policies often limit coverage for war or acts of terrorism and, even where they cover terrorist activity by individuals or political groups, policies may exclude coverage for acts of government or government-sponsored organizations. This may be particularly problematic in the cyber context where cyberspace has recently been deemed a warfare "domain" by the United States government.[221] Numerous recent reports have discussed the allegations of government-sponsored hacking by China, North Korea, Russia, and other countries, including into U.S. government agencies and major corporations.[222] One report identified as many as 141 distinct entities or organizations that had breaches of cybersecurity at the hands of the Chinese army in the last seven years.[223] The Office of the Secretary of Defense has publicly accused the Chinese government of conducting cyber espionage,[224] and the U.S. Department of Justice has indicted five Chinese military officers,

---

221. Jim Garamone, *Cybercom Chief Discusses Importance of Cyber Operations*, U.S. DEP'T OF DEFENSE (Apr. 14, 2015), www.defense.gov/News-Article-View/Article/604453/cybercom-chief-discusses-importance-of-cyber-operations.

222. *See, e.g.*, Chris Strohm, *No Sign China Has Stopped Hacking U.S. Companies, Official Says*, BLOOMBERG TECH. (Nov. 18, 2015), www.bloomberg.com/news/articles/2015-11-18/no-sign-china-has-stopped-hacking-u-s-companies-official-says ("The Chinese government hasn't stopped hacking American companies to steal industrial trade secrets, despite pledges to do so, the top U.S. national counterintelligence official said[.]"); *China Suspected in Massive Breach of Federal Personnel Data, AP,* June 4, 2015 ("China-based hackers are suspected of breaking into the computer networks of the U.S. government personnel office and stealing identifying information of at least 4 million federal workers, American officials said Thursday."); Evan Perez & Shimon Prokupecz, *How the U.S. Thinks Russians Hacked the White House*, CNN, Apr. 8, 2015, www.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/; Bob Orr, *Why the U.S. was Sure North Korea Hacked Sony*, *CBS NEWS*, Jan. 19, 2015, www.cbsnews.com/news/why-the-u-s-government-was-sure-north-korea-hacked-sony/; *FBI's James Comey Accuses China of Hacking into Every Major American Company*, INDEPENDENT (Oct. 6, 2014), www.independent.co.uk/news/business/news/fbis-james-comey-accuses-china-of-hacking-into-every-major-american-company-9777587.html ("[FBI Director] James Comey says there are two types of American companies: those that have been hacked and those that don't know it yet[.]").

223. David E. Sanger, David Barboza & Nicole Perlroth, *Chinese Army Unit Is Seen as Tied to Hacking Against U.S*, N.Y. TIMES, Feb. 18, 2013, at A1.

224. *See* OFFICE OF SECRETARY OF DEFENSE, ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA 2013, archive.defense.gov/pubs/2013_China_Report_FINAL.pdf; *see also* Shannon Tiezzi, *China (Finally) Admits to Hacking* (Mar. 18, 2015), http://thediplomat.com/2015/03/china-finally-admits-to-hacking/.

alleging they hacked U.S. companies' computers to steal trade secrets.[225] Given the significance of this threat, cyber policies should be reviewed to ensure that coverage for government-sponsored cyber roles is not excluded.

[M] Other Exclusions

Cyber policies often contain important exclusions that substantially narrow coverage. For example, some cyber policies exclude damage to computers and related business interruption on the theory that these risks should be covered by a more traditional property policy, at least when due to natural causes.[226] Cyber policies may also exclude securities claims,[227] but a cyber breach involving a company's confidential financial information may be among its most important risks. Employment claims are also excluded under certain cyber policies, though the disclosure of confidential information about employees is an important risk for many companies.[228] Insurers may also argue that antitrust exclusions are implicated where information is stolen or disclosed for anticompetitive purposes.

Another important exclusion may concern business interruption. Some policies specifically exclude business interruption due to a cyber breach. Others specifically provide that coverage.[229] An insured should evaluate the potential impact of cyber losses on its ability to conduct business and determine whether business interruption for this kind of loss is necessary or appropriate.

Exclusions barring coverage for liability assumed under contract or agreement are also increasingly important in the cyber context. The potential role of the contract exclusion is illustrated by the recent

---

225. Devlin Barrett & Siobhan Gorman, *U.S. Charges Five in Chinese Army with Hacking*, WALL ST. J., May 19, 2014, http://online.wsj.com/news/articles/SB10001424052702304422704579571604060696532.

226. *See, e.g.*, Philadelphia Insurance Co. Cyber Security Liability Coverage Form PI-CYB-001, § IV.C (2010) (excluding from loss expenses arising out of "fire, smoke, explosion, lightning, wind, flood, earthquake, volcanic eruption . . . or any other physical event or peril"); *see also* CHUBB CyberSecurity Form 14-02-14874, § III.C.6 (2009) (excluding from loss any expense "resulting from mechanical failure, faulty construction, error in design, latent defect, wear or tear, gradual deterioriation").

227. *See, e.g.*, Philadelphia Insurance Co. Cyber Security Liability Coverage Form PI-CYB-001, § IV.R (2010) (excluding from coverage violations of the Securities Exchange Act).

228. *See, e.g.*, Philadelphia Insurance Co. Cyber Security Liability Coverage Form PI-CYB-001, § IV.L (2010) (excluding from coverage employment practices or discrimination claims).

229. *See, e.g.*, Travelers Cyber Risk Form CYB-3001, § I.J (2010) ("The Company will pay the Insured Organization for Business Interruption Loss incurred by the Insured Organization which is directly caused by a Computer System Disruption taking place during the Policy Period[.]").

decision denying P.F. Chang's claim for coverage under a Chubb CyberSecurity policy.[230] The case involved a data breach in which over 60,000 of the restaurant chain's customers' credit card numbers were allegedly compromised.[231] The insurer reimbursed its insured for certain costs incurred in conducting a forensic investigation into the data breach and the costs of defending litigation filed by third parties whose credit card information was stolen—costs commonly covered under cyber policies. Chubb, however, denied coverage for amounts the insured owed to its credit card servicer under their master service agreement (MSA), which included:

(1) reimbursement of fraudulent charges on the stolen credit cards;

(2) the costs to notify cardholders affected by the breach and to reissue new cards to those individuals; and

(3) a flat fee relating to P.F. Chang's compliance with Payment Card Industry Data Security Standards (PCI DSS).[232]

In addition to holding that the fees to the credit card servicer did not trigger coverage under the policy's definition of a "Privacy Injury,"[233] the court held that coverage was barred under two exclusions precluding coverage for contractual obligations assumed by the insured.[234] In support of this, the court cited the MSA between the insured and its credit card servicer, which required the insured to reimburse the servicer for the fees the servicer incurred (for example, reimbursement of fraudulent charges, notification costs).[235]

Credit card arrangements are often covered by specific provisions in cyber policies. Insureds that process credit card transactions as a part of their business should give particular attention to these provisions and should consider cyber policies that explicitly include this coverage.[236]

---

230. P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co., 2016 WL 3055111 (D. Ariz. May 31, 2016).
231. *Id.* at *1–2.
232. *Id.*
233. *Id.* at *4–5. The court held that there was no "Privacy Injury," because that term was defined to "injury sustained or allegedly sustained by a Person because of actual or potential unauthorized access to such Person's Record, or exceeding access to such Person's Record." *Id.* at *4. Since the lost credit card information belonged to the customers' themselves—not the credit card servicer that brought suit against P.F. Chang's—there was no injury sustained by a Person because of unauthorized to "*such* Person's record." *Id.*
234. *Id.* at *7–8.
235. *Id.* at *8.
236. *See, e.g.*, AIG, Specialty Risk Protector, CyberEdge Security and Privacy Liability Insurance, Security and Privacy Coverage Section, at 2(h), 2(j) (2013)

[N] Physical Impact from a Cyber-Attack

With the ever-increasing "Internet of things,"[237] the availability of devices prone to cyber-attacks continues to grow on a daily basis. Coupled with this is the growing threat of physical damage caused by a cyber-attack. For example, a hacker could attack a manufacturer's operating system, causing a breakdown in equipment. While few such incidents have been widely reported, they are no longer restricted to science fiction or the movies.[238] Policyholders at risk of suffering physical damage from a cyber-attack need to assess their coverage, since many cyber policies exclude third-party liability coverage for bodily injury and property damage,[239] and traditional coverages increasingly include their own cyber-related exclusions.[240]

(defining "Loss" to include "amounts payable in connection with a PCI-DSS Assessment," which is in turn is defined as "any written demand received by an Insured from a Payment Card Association . . . or bank processing payment card transactions . . . for a monetary assessment (including a contractual fine or penalty) in connection with an Insured's non-compliance with PCI Data Security Standards which resulted in a Security Failure or Privacy Event"), www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-wording-sample-specimen-form.pdf .

237. "The Internet of Things (IoT) is a computing concept that describes a future where everyday physical objects will be connected to the Internet and be able to identify themselves to other devices." *Internet of Things (IoT)*, TECHOPEDIA, www.techopedia.com/definition/28247/internet-of-things-iot (last visited Aug. 17, 2016).

238. *See, e.g.*, Lucy L. Thomson, *Cyber Physical Risk*, ABA Litigation Section Insurance Coverage Litigation Committee, at 7–12 (2016) (discussing attacks ranging from the disabling of a computer system designed to detect pipeline leaks (that caused a major oil spill and loss of life) to a hacking incident causing four trains to derail); *see also* LLOYD'S EMERGING RISK REPORT 2015, BUSINESS BLACKOUT: THE INSURANCE IMPLICATIONS OF A CYBER ATTACK ON THE US POWER GRID (2015) (describing the severe potential implications of a hypothetical attack on a "smart" power grid, resulting in a widespread blackout across the Northeast, leaving millions without power and shutting down phone systems, Internet, television, traffic signals, factories and commercial activity for several days), www.lloyds.com/~/media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf; What Every CISO Needs to Know About Cyber Insurance, at 2 (Symantec White Paper 2015) ("Experts are telling us we could experience a massive cyber terrorist event that could cause major market disruptions, and even physical damage to property and critical infrastructure."), www.symantec.com/content/dam/symantec/docs/white-papers/what-every-ciso-needs-to-know-cyber-insurance-en.pdf

239. *See, e.g.*, note 226 and accompanying text.

240. *See, e.g.*, notes 30–31 *supra* and accompanying text; *see also* Institute Cyber Attack Exclusion Clause (CL 380) (Oct. 11, 2003) ("in no case shall this insurance cover loss damage liability or expense directly caused by or

One option for filling this potential gap in coverage may be cyber difference-in-conditions (DIC) coverage, which is now offered by several insurers and generally provides coverage for perils excluded under other policies.[241] Policyholders should work closely with their information technology professionals, brokers, risk managers, and attorneys to review their existing scope of coverages and the potential need for DIC cyber insurance.

§ 16:3.3 SEC Disclosure and Other Regulatory Initiatives

Insurance for cyber risks, and an understanding of such insurance, takes on additional significance in the wake of guidance issued by the SEC on October 13, 2011.[242] This guidance requires publicly traded companies to disclose, among other things:

- risk factors relating to a potential cyber incident, including known or threatened attacks;
- costs and other consequences associated with known cyber incidents or risks of potential incidents;
- material legal proceedings involving cyber incidents; and
- insurance for cyber risks.[243]

These requirements underscore the need for cyber insurance and a clear understanding of what such policies cover, as failure to make disclosures could potentially subject registrants to SEC enforcement action and shareholder suits.[244]

---

contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any electronic system").

241. *See, e.g., Cyber Coverage & Services*, AEGIS (offering a difference-in-conditions option "which wraps coverage around existing policies, i.e., property, casualty, terrorism and environmental" and "delivers full cyber coverage for physical damage, bodily injury and environmental issues"), www.aegislink.com/aegislink/services/underwriting/products/cyber-coverage-and-services.html (last visited Aug. 17, 2016); AIG CyberEdge PC (Apr. 2014 (offering umbrella difference-in-conditions coverage for, inter alia, property damage)), www.aig.com/content/dam/aig/america-canada/us/documents/business/cyber/cyberedge-pc-product-profile-final.pdf.

242. *CF Disclosure Guidance: Topic No. 2, Cybersecurity, U.S. Sec. & Exch. Comm'n* (Oct. 13, 2011), www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

243. *Id*.

244. *See* section 16:2.3[A], *supra*.

As noted above, the SEC has emphasized that cybersecurity and board of director responsibilities in this area will be a principal focus of law enforcement efforts.[245]

In addition to the SEC, other federal government agencies have increased their focus on cyber insurance–related issues. As noted above, the FTC has become active and aggressive in this area.[246] The Department of Homeland Security, for example, convened a Cybersecurity Insurance Workshop in 2012 to discuss pricing, insurable risks, and challenges associated with cyber insurance.[247] The White House identified a cybersecurity policy coordinator, convened a multidisciplinary group on cybersecurity-related jobs (including insurance industry positions), and issued an executive order on cybersecurity risks.[248] The resultant executive order was entitled "Improving Critical Infrastructure Cybersecurity" and directed the National Institute of Standards and Technology to develop a voluntary cybersecurity framework.[249] These efforts have continued to result in new initiatives and scrutiny on cybersecurity.[250] Governmental activities at the state, federal, and international levels will continue to evolve and may have an impact on the availability of insurance products and government requirements for cyber insurance. For example, on the international stage, the European Union and the United States have agreed to, but

---

245. Comm'r Luis A. Aguilar, Address at Cyber Risks and the Boardroom Conference: Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening Focus (June 10, 2014); *see also supra* section 16:3.2[F].

246. *See* note 147, *supra*.

247. *See* U.S. DEP'T OF HOMELAND SEC., NAT'L PROTECTION & PROGRAMS DIRECTORATE, CYBERSECURITY INSURANCE WORKSHOP READOUT REPORT (Nov. 2012), www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf.

248. *See White House Author Michael Daniel*, WHITE HOUSE BLOG, www.whitehouse.gov/blog/author/michael-daniel (last visited Aug. 17, 2016); *see also* Press Release, AccessWire, Innovation Insurance Group President Participates in Cyber "Jobs of the Future" Event at White House (June 5, 2012), www.innovationinsurancegroup.com/images/IIG-ISA_WH_Security_Workplace_Event_Press_Release_6-4.pdf; Press Release, White House, Exec. Order—Improving Critical Infrastructure Cybersecurity (Feb. 19, 2013), www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

249. *See Cybersecurity Framework*, NAT'L INST. OF STANDARDS & TECH. (Aug. 17, 2016), www.nist.gov/cyberframework/.

250. *Assessments: Cyber Resilience Review (CRR)*, U.S. COMPUTER EMERGENCY READINESS TEAM [US-CERT], www.us-cert.gov/ccubedvp/self-service-crr (last visited Aug. 17, 2016); *National Protection and Programs Directorate*, DEP'T OF HOMELAND SEC. (June 27, 2016), www.dhs.gov/national-protection-and-programs-directorate; *see, e.g.*, Mark A. Hofmann, *Senate Panel Takes Up Cyber Insurance Issues*, BUS. INS., Mar. 19, 2015, www.businessinsurance.com/article/20150319/NEWS06/150319798.

have not yet finalized, the EU-U.S. Privacy Shield that will impose more regulations on U.S. companies to protect the personal information of Europeans.[251]

251. *See* Julia Fioretti, *EU, United States Agree on Changes to Strengthen Data Transfer Pact*, REUTERS (June 24, 2016), www.reuters.com/article/us-eu-dataprotection-usa-idUSKCN0ZA1QT.