An excerpt from:

Minnesota CLE's: **Minnesota Insurance Law Deskbook**

CHAPTER 26

CYBER INSURANCE

AUTHORS:

BENJAMIN A. JOHNSON
JOHNSON & LINDBERG PA
BLOOMINGTON

KATIE C. PFEIFER
DORSEY & WHITNEY
MINNEAPOLIS

Table of Contents

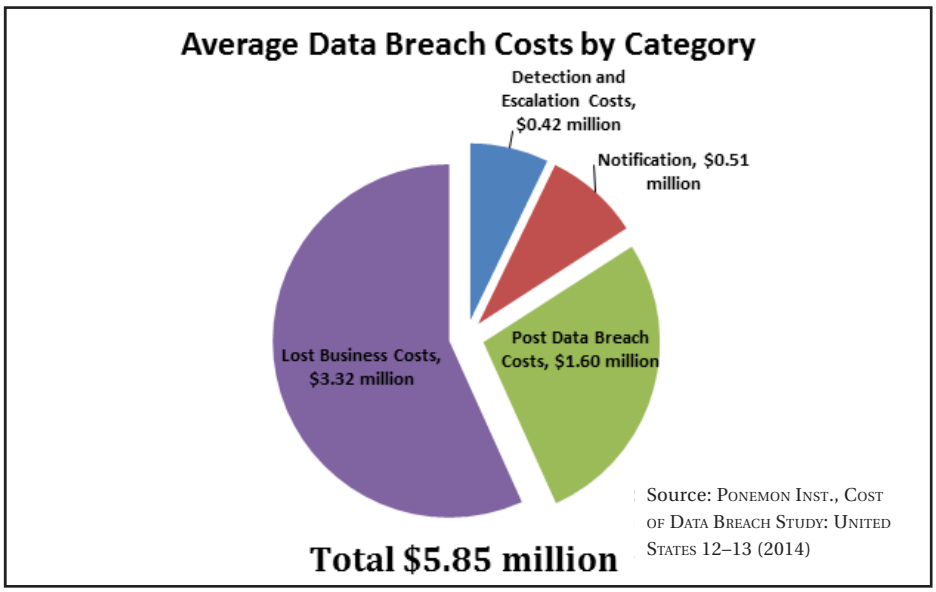
§ 26.1 OVERVIEW OF CYBER LIABILITY

Coverage issues related to cyber liability began arising around 25 years ago. *See, e.g.*, *Magnetic Data v. St. Paul & Marine Ins. Co.*, 442 N.W.2d 153 (Minn. 1989) (concluding that erasure of magnetically encoded data on a computer disk was not insured). Insurance companies responded by offering specialty coverage for cyber liability and data breaches over a decade ago. For much of the time since, cyber insurance has remained obscure. It was not until high profile data breaches in the early 2010s that a significant number of companies begin considering purchasing cyber insurance. *See*, *e.g.*, Shane Richmond & Christopher Williams, *Millions of Internet Users Hit by Massive Sony PlayStation Data Theft*, THE TELEGRAPH, Apr. 26, 2011, *available at* <www.telegraph.co.uk/technology/news/8475728/Millions-of-internet-users-hit-by-massive-Sony-PlayStation-data-theft.html>. Perhaps because of the recentness of this trend, the law surrounding cyber insurance remains undeveloped.

Federal statute defines "data breach" as "the loss, theft, or unauthorized access … to data containing sensitive personal information, [in] electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data." 38 U.S.C. § 5727(4). Despite attention-grabbing headlines, (e.g., Steven Alexander & Jennifer Bjorhus, *Target Says Breach May Affect 40 Million Credit, Debit Cards*, STAR TRIBUNE, Dec. 20, 2013, *available at* <www.startribune.com/business/236443001.html>), most data breaches are not "mega-breaches," i.e., breaches of over 100,000 records. *See* PONEMON INSTITUTE, 2014 COST OF DATA BREACH STUDY: UNITED STATES, 1 (2014). Nevertheless, companies affected by data breaches incur significant costs. Between 2005 and 2014, responding to a data breach cost an average of around $5.85 million. *Id.* at 6. During the same period, the average cost for each record exposed was around $194. *Id.* at 7. The average cost per record ranges widely between industries. For example, in 2013, data breaches in the healthcare sector averaged $316 per record, and breaches in the research sector averaged $75 per record. *Id.* at 7 fig. 4.

Although most people associate data breaches with a malicious or criminal attack, many data breaches have other causes. Criminal or malicious attacks account for 44 percent of data breaches; system failures account for 31 percent of data breaches; and human error accounts for 25 percent of data breaches. *Id.* at 8. These distinctions are important because the cause of the data breach affects the availability of coverage.

The type of costs for which the insured seeks indemnity also affects coverage. Costs for data breaches generally fall into four categories: (1) detection and escalation expenses, (2) notification costs, (3) post data breach costs, and (4) lost business expenses. *Id.* at 12–13.



The first category of costs—detection and escalation costs—include expenses for forensics and investigation, audits, managing employees' response, and communicating about the breach internally. *Id.* Detection and escalation costs are typically incurred in the immediate aftermath of the breach when the victim assesses the scope of the data breach. For example, the victim will investigate what IT infrastructure was affected, what information was exposed, and what software was compromised. Similarly, these costs are incurred when the company investigates the underlying cause of the breach. This assessment may include a technical evaluation of vulnerabilities and an operational evaluation of the environment that allowed vulnerabilities to arise.

The second category of costs is notification costs. *Id.* These costs arise from companies' efforts to notify those affected by a breach. State and federal law often govern the scope and content of external notifications. *See, e.g.*, MINN. STAT. § 325E.61 (requiring disclosure of breach of security involving defined personal information in certain circumstances); 45 C.F.R. §§ 164.400–164.414 (requiring notification after the breach of protected health information). Those requirements are likely to grow and place additional burdens on companies following a data breach. Michael D. Shear & Natasha Singer, *Obama to Call for Laws Covering Data Hacking and Student Privacy*, NEW YORK TIMES, Jan. 11, 2015 *available at* <www.nytimes.com/2015/01/12/us/politics/obama-to-call-for-laws-covering-data-hacking-and-student-privacy.html?_r=0>. In addition to ensuring compliance with these laws, notification requires compiling a database of affected individuals, and drafting and distributing the notification. Therefore, notification costs include expenses for legal and consulting services, generating a data base of affected individuals, and mailings. 2014 COST OF DATA BREACH STUDY at 12–13.

The third category of costs is post-breach expenses, specifically, costs related to fielding incoming communications, credit monitoring, remedial work, and defending against and paying legal claims. *Id.* at 13. Post-breach costs may also include costs for restoring or regenerating lost data.

The fourth and final category of costs is typically the highest: lost business. *Id.* Lost business costs result from the negative effects data breaches have on a company's reputation. *Id.* These reputational

harms lead to lost customers and increased costs of acquiring new customers. *Id.* Over the last nine years, companies suffering data breaches incurred on average over $3.5 million in lost business expenses after the breach. *Id.* at 13 fig. 14.

The remainder of this chapter focuses on whether, and in what circumstances, various insurance policies provide coverage for these costs. The first section focuses on coverage for data breaches under traditional insurance policies. The second section discusses coverage under cyber insurance policies.

§ 26.2 POTENTIAL SOURCES OF INSURANCE RECOVERY

A. Traditional Insurance Policies: First-Party Coverage

First-party losses occur when an insured loses the use of its own property because of damage or destruction. In the area of cyber insurance, such a loss generally occurs when an outside entity or an unauthorized internal user breaches the security protections on an insured's computer or computer network. It may occur in the form of an unseen infiltration through hacking, malware, viruses, etc., or in the form of fraud. As noted above, it may also be the result of system failures or human error by authorized internal users.

Costs connected to first-party coverage can fall into all four of the categories discussed above. More specifically, there are direct damages including replacement of corrupted data, labor expenses for re-entering data, the loss of stolen property, and the cost of replacing inoperable systems; consequential damages including the loss of income and administrative costs for dealing with the crisis; and regulatory costs associated with reporting data breaches under state and federal regulations, paying fines or other penalties, and defense costs connected to those fines.

Insureds without a specific cyber insurance policy providing coverage for these types of losses generally seek coverage from property insurance policies and crime insurance policies.

1. Property Insurance

Property damage generally includes physical injury to tangible property, including all resulting loss of use of that property, and also loss of use of tangible property that is not physically injured. The primary question regarding property damage is whether loss or damage to electronic data is a "direct physical loss." Both property insurance and commercial general liability (CGL) policies include coverage for physical losses to tangible property. Property insurance generally provides first-party coverage, while CGL policies provide third-party coverage. Because both deal with losses to tangible property, cases involving claims under either type of policy are helpful in understanding what claims could constitute a property loss. The largest debate under both types of coverage is whether electronic data is tangible property.

NOTE

Hewlett-Packard Co. v. Factory Mutual Insurance Co., No. 04 CIV. 2791, 2007 WL 983990 (S.D.N.Y. Mar. 30, 2007) did not involve an interpretation of the term "tangible property," but shows an example of a true first-party claim. In that case, a Hewlett-Packard (HP) employee sabotaged the efforts to build a database, which delayed putting a new computer server on the market. HP applied to its insurer to recover for property damage to the database and for loss of sales. Factory Mutual raised several arguments to coverage, but the court rejected them all.

A 1983 case, *Centennial Insurance Co. v. Applied Health Care Systems, Inc.*, 710 F.2d 1288 (7th Cir. 1983), involved a computerized data processing service that purchased controllers from Microcomputer Technology, Inc. (MCT). The controllers allegedly malfunctioned and the processing service sued MCT. MCT tendered the defense to its insurer, but the insurer denied coverage and refused to defend. While the district court and parties spent time discussing the question of whether "information stored in a data processing system may be fairly characterized as tangible property," the court of appeals declined to answer that question. *Centennial Ins.*, 710 F.2d at 1291 n.7. Instead, the court focused on the duty to defend and determined that there was a duty because the complaint "clearly raises the specter that liability for property damage may ensue." *Id.* at 1291.

In 1989, the Minnesota Supreme Court also declined to address the issue, saying "[w]e need not determine, however, whether the computer information is intangible or tangible property." *Magnetic Data*, 442 N.W.2d at 156. By the early 1990s, though, courts began to address the question of whether electronic data constitutes tangible property. A 1991 case from Minnesota concerned computer tape and the data on the tape. The court compared the tape to motion picture film and found that the data was tangible property because it was "integrated completely with the physical property of the tape." *Retail Sys., Inc. v. CNA Ins. Cos.*, 469 N.W.2d 735, 737 (Minn. Ct. App. 1991).

As time passed, courts began to shift their position. An Oklahoma court determined that the loss of electronic data did not constitute property damage in *State Auto Property & Casualty Insurance Co. v. Midwest Computers & More*, 147 F. Supp. 2d 1113 (W.D. Okla. 2001). Midwest Computers & More provided services to a business, and the business claimed that as a result of the services, the business lost the use of the computers and lost extensive amounts of data that was stored on the computer system. The court addressed the questions of whether the computer data, allegedly destroyed, constituted tangible property and whether the loss of use of a computer occurred and constituted property damage. On the first question, the court found that computer *data* had no physical substance and was therefore not tangible property. The court then found that the claim of loss of use of a computer (*hardware*) did constitute property damage, but that the claim in the suit was prohibited under the "your work" exclusion in the policy.

In *NMS Services, Inc. v. The Hartford*, 62 F. App'x 511 (4th Cir. 2003), an NMS employee installed two hacking programs on NMS's system. After he was fired, he used the programs to erase vital computer files and databases. NMS made a claim with Hartford under both the special property coverage form and a computer and media endorsement. Hartford denied the claim, arguing that a dishonesty exclusion precluded coverage because NMS had entrusted the employee with its property.

The exclusions in both the special property coverage form and the endorsement prohibited coverage for dishonest or criminal acts by employees. But the special property coverage form specifically said that it did provide coverage for acts of destruction by employees. The court found that the special property coverage applied, but the endorsement did not. Based on that finding, the court found that there was coverage for lost business income, extra expenses for costs incurred in the restoration period, and because the data lost was a valuable paper or record, the cost to restore that data. A dissent argued that the computer and media endorsement amended the policy in such a way as to exclude coverage.

Later in 2003, the Fourth Circuit addressed the issue of whether computer data and software systems were "tangible" property in *America Online, Inc. v. St. Paul Mercury Insurance Co.*, 347 F.3d 89 (4th Cir. 2003). The case involved a class action suit by America Online (AOL) customers who alleged that a new version of the AOL software damaged their computers by altering their existing software, disrupting network connections, destroying stored data, and triggering operating system crashes. The insurer denied coverage under a CGL policy, arguing that the claimed damages did not constitute property damage. AOL argued that there was damage to tangible property because (1) there was an allegation of damage to computers, (2) software involves the arrangement of atoms on computer disks and therefore has a physical component, and (3) the definition of "tangible" in the policy was ambiguous and should be construed in AOL's favor. The court determined that the physical magnetic material on the hard drive, the arrangement of atoms on a computer disk, was tangible property. However, that conclusion did not mean that the data or information stored in such a manner was, itself, tangible property. The court distinguished between damage to the software and damage to the hardware. The court concluded that the magnetic material on the hard drive, the software, could be reordered by reinstalling programs and reentering data, but that did not affect the "physical capabilities and properties of the hard drive." *Am. Online*, 347 F.3d at 95. The court determined that the losses identified—those to the software rather than the hardware—amounted to the loss of an abstract idea, logic, instruction, or information. Therefore, it did not constitute physical damage to tangible property.

Also in 2003, the Minnesota Court of Appeals found that data was not tangible property. In an unreported case, the court relied on the *Black's Law Dictionary* definition of "tangible property" and concluded that data was information and, therefore, "data may not reasonably be interpreted as 'tangible property.'" *Compaq Computer Corp. v. St. Paul Fire & Marine Ins. Co.*, No. C3-02-2222, 2003 WL 22039551, at *8 (Minn. Ct. App. Sept. 2, 2003).

Eyeblaster, Inc. v. Federal Insurance Co., 613 F.3d 797 (8th Cir. 2010) is another case involving the application of Minnesota law. The case involved a CGL policy, but looked to the definition of "property." At issue was a claim by a computer user who alleged that his computer, software, and data were damaged after he visited an Eyeblaster website. The fact that the computer froze, worked slowly, and ran the risk of transferring a virus to other computers led the court to conclude that there was damage in the loss of use of the computer, despite the fact that it was not physically injured.

Together, these cases show that there may be room to make a claim under some first-party property insurance policies. However, where the only claimed damage involves the loss of electronic data, courts likely will find that the data is not tangible property.

PRACTICE TIP

In any claim under a property insurance policy, the first step should involve identifying the type of damages claimed. If there is no claim of damage to hardware, there likely will be no coverage.

2. Crime Insurance

Businesses often purchase blanket crime policies. Those policies, sometimes called fidelity insurance, provide coverage for items including employee theft, forgery, theft of money, funds transfer fraud, and computer fraud. The ISO crime coverage form, CR 00 07, states that the insurer will pay for loss of, or damage to, money, securities, and other property resulting directly from the use of any computer to fraudulently transfer that property from inside the premises or bank to a person or place outside the premises. Coverage for computer fraud often turns on the same questions of the definition of "property" that appear in both first-party property coverage and CGL coverage. That is, where the loss involves data, there is often a dispute over whether an item constitutes tangible property. *See Peoples Tel. Co. v. Hartford Fire Ins. Co.*, 36 F. Supp. 2d 1335 (S.D. Fla. 1997).

Coverage for computer fraud under a crime policy can also turn on the questions of whether the theft involved insured property and whether the computer fraud was the proximate cause of the loss. In *Retail Ventures, Inc. v. National Union Fire Insurance Co. of Pittsburgh, Pa.*, 691 F.3d 821 (6th Cir. 2012), DSW Shoe Warehouse, Inc., was involved in a hacking scheme that compromised customer credit card and checking account information. DSW and its parent company sustained significant losses and incurred expenses connected to an FTC investigation, charge backs for purchases made with the stolen information, card replacement for customers, and account monitoring. The policy in question covered losses resulting directly from the theft of any insured property by computer fraud, and applied to property located on the premises of the insured. In dicta, the court raised the question of whether the information was property owned by, held in some capacity by, or for which DSW was legally liable. The court did not address that question, though, because the insurer did not raise the issue. Instead, the insurer disputed whether the loss resulted directly from the theft. The insurer argued that a loss resulting directly from computer fraud required that the theft of property be the sole and immediate cause of the insured's loss. Because DSW's loss was connected largely to the use of stolen credit card information that actually belonged to its customers, the insurer argued that DSW's losses were not DSW's own loss. The court noted that there was a split in interpretation among various state and federal courts. The court acknowledged that the policy in question was a commercial crime policy directed at the insured's loss, as opposed to a commercial liability policy, but found that the phrase "resulting directly from" was ambiguous. On that interpretation, the court concluded that the losses DSW sustained were covered. *Cf, Tooling, Mfg. & Technologies Ass'n v. Hartford Fire Ins. Co.*, 693 F.3d 665, 673–76 (6th Cir. 2012) (discussing the split between the "direct-is-direct" approach and the "proximate cause" approach in determining whether a loss is covered); *Cargill, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh*, No. A03-187, 2004 WL 51671, at *12 (Minn. Ct. App. Jan. 13, 2004) ("We conclude that the provision unambiguously covers only Cargill's direct losses, not claims arising from a third party's direct losses, and requires that the insured's loss—and not the third party's claim—be directly caused by employee theft in order for coverage to become available.").

Another question of coverage under a crime policy has to do with what use is covered. Computers have become ubiquitous, and many routine actions by businesses involve the use of a computer. Therefore, parties often dispute the meaning of the phrase "use of any computer" that appears in the standard policy language. Insureds seek coverage for any loss connected to a computer use, while insurers typically argue that the use applies to actions like hacking. Court decisions have followed both arguments.

Brightpoint, Inc. v. Zurich American Insurance Co., No. 1:04-CV-2085-SEB-JPG, 2006 WL 693377 (S.D. Ind. Mar. 10, 2006) involved the use of a fax machine. The insured, Brightpoint, sold prepaid phone cards. Brightpoint sold those phone cards to a dealer who paid through the use of post-dated checks; the dealer would fax copies of the checks with purchase orders before receiving the phone cards. During one such transaction, someone faxed fraudulent documents and received the phone cards without any payment actually being made. Brightpoint notified the insurer of the loss and sought recovery under the computer crime provision.

The insurer denied coverage, arguing that Brightpoint did not own the cards, the cards were not transferred from Brightpoint's premises, the cards were not covered property, and there was no evidence that a computer was used to fraudulently cause a transfer of the phone cards. The court determined that coverage exclusions did apply because, in part, the actual transfer of the phone cards was made following a face-to-face meeting, not based on the facsimile transmission. Therefore, the use of the computer did not cause the loss. Even though the court ultimately determined that the use of a fax machine is not what caused the loss and the opinion did not directly answer the question of whether the fact that communications between the criminal and the insured occurred through the use of faxes constituted "use of any computer," the case has been cited by insureds to claim that crime resulting from any use of a computer, even normal business use, is covered under the crime policy.

The *Brightpoint* case received attention in *Owens, Schine & Nicola, P.C. v. Travelers Casualty & Surety Co. of America*, No. CV095024601, 2010 WL 4226958 (Conn. Super. Ct. Sept. 20, 2010). In that case, a law firm purchased a crime insurance policy from Travelers that included coverage for computer fraud. The law firm reported that it was contacted by an attorney in another state who wanted help on a collection matter for a client located in China. All of the communication was by email. The firm received what it believed to be a check from the debtor, deposited the check in the firm's trust account, and then wired the funds to the client. The firm later discovered that the check was fraudulent, but the firm's bank had already made the payment. Travelers denied coverage, arguing that the loss did not result from computer fraud which, according to Travelers, meant an incident that amounted to hacking. The fact that communication was through email, Travelers argued, was not enough to prove that the loss was the result of the use of a computer. The court found that the language in the policy discussing "use of a computer" was ambiguous and could be interpreted to mean more than a hacking incident. The fact that the crime occurred through the use of email was sufficient to support a claim for coverage that survived summary judgment.

More recently, a decision out of New York adopted the position Travelers proposed in the *Owens* case. In *Universal American Corp. v. National Union Fire Insurance Co. of Pittsburgh, Pa*, 110 A.D.3d 434 (N.Y. App. Div. 2013), the appellate division upheld the decision of a lower court which found that coverage for loss from a fraudulent entry of electronic data applied to wrongful acts like hacking, and not for fraudulent entries made by parties who, while authorized to use a computer system, did so

to seek reimbursement for health care services that were not actually provided. The decision formed the basis for the conclusion of a California court in *Pestmaster Services, Inc. v. Travelers Casualty & Surety Co. of America*, No. CV 13-5039-JFW, 2014 WL 3844627 (C.D. Cal. July 17, 2014). The decision in the New York case is on appeal.

PRACTICE TIP

In crime insurance claims, the specific policy language, if any, defining "use of a computer" will likely determine if coverage exists under the facts of the case.

B. Traditional Insurance Policies: Third Party

Third-party losses are losses that result when someone accesses the insured's electronic data and destroys it, damages it, or steals the information of some third party when that information is in the care and control of the insured. Losses generally involve a theft of personal information, transmission of a computer virus from the insured's system to some third party's system, exclusion of an authorized third party from accessing the insured's computer system, or failing to give notice of an intrusion or theft to a third party in violation of statutes, regulations, or contractual terms.

Costs fall into two primary categories. First, an insured may be responsible for a third party's loss of data, hardware, and software. Like a first-party claim, the losses would generally include replacement of corrupted data, labor expenses for re-entering data, the loss of stolen property, and the cost of replacing inoperable systems. Second, there are the more widely publicized claims connected to the theft of personal information. Those costs and claims may be based on providing required notice to a third party, repairing identity theft, monitoring credit reports, and invasion of privacy. In addition to or in the absence of cyber insurance, insureds have several options that they can look to for potential coverage for these types of claims.

1. CGL Policies

Insurance claims arising out of third-party claims are generally made under CGL policies. Insureds have made claims under CGL policies under both "Coverage A" and "Coverage B." Coverage A typically says that the insurer will pay those sums that the insured becomes legally obligated to pay as damages because of bodily injury or property damage, while Coverage B applies to personal and advertising injury, which includes "publication, in any manner, of material that violates a person's right of privacy."

a. Coverage A

Coverage A under a standard CGL policy covers bodily injury or property damage. Bodily injury includes injury, sickness, or disease, while property damage includes physical injury to tangible property and loss of use of tangible property.

Claims by third parties for bodily injury sustained as the result of computer fraud are extremely difficult to support. In some jurisdictions, plaintiffs have asserted claims for emotional distress

or mental anguish. Not every jurisdiction requires a physical component to a claim for emotional distress damages. Under Minnesota law, though, it is difficult to envision a scenario in which a case involving computer fraud would support a claim for emotional distress damages. *See Lickteig v. Alderson, Ondov, Leonard & Sween, P.A.*, 556 N.W.2d 557, 560 (Minn. 1996) (limiting emotional distress damages to three circumstances: (1) where the plaintiff suffers a physical injury and has accompanying mental anguish; (2) where there has been a "direct invasion of the plaintiff's rights such as that constituting slander, libel, malicious prosecution, seduction or other willful, wanton or malicious conduct"; or (3) where it is part of the stand-alone tort of intentional infliction of emotional distress).

The more likely claim under Coverage A would relate to property damage. As discussed in detail above, where claims involve only the claim of lost data, the national trend is to conclude that the data is not tangible property and, therefore, there is no coverage. *See, e.g., Cincinnati Ins. Co. v. Prof'l Data Servs., Inc.*, No. CIV. A. 01-2610-CM, 2003 WL 22102138, at *6–7 (D. Kan. July 18, 2003).

CAVEAT

The issue of whether there is coverage under Coverage A is likely to become moot in the coming years. In 2001, the Insurance Services Office (ISO) changed the definition of "property damage." The definition now states that "electronic data is not tangible property." It adds that electronic data includes "information, facts or programs stored as or on, created or used on, or transmitted to or from computer software." Similarly, the standard ISO policy also added an electronic data exclusion in 2004. That exclusion, known as "exclusion p," states that the policy does not cover "[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." As a result of the changes, disputes regarding whether electronic data is tangible property under a CGL policy should become rare.

b. Coverage B

Coverage B in a standard CGL policy says that the insurer "will pay those sums that the insured becomes legally obligated to pay as damages because of 'personal and advertising injury.'" As most relevant to cyber liability issues, personal and advertising injury includes "[o]ral or written publication, in any manner, of material that violates a person's right of privacy." (Also covered as "personal and advertising injury" is "[o]ral or written publication, in any manner, of material that slanders or libels a person or organization or disparages a person's or organization's goods, products or services[.]") Claims under this provision typically involve alleged damages due to the theft of personal information from a large company, like the well-publicized data breaches involving Target, Sony, and others.

There are several significant issues connected to claims made under Coverage B. For example, several general exclusions in the CGL policy might apply. Exclusions for intentional or criminal acts are not unique to these claims; if there is evidence that an insured committed such an act, an insurer may dispute coverage. Similarly, where there is evidence of a knowing violation of the rights of another, coverage may be excluded. Exclusions dealing with intellectual property may also apply.

Outside of policy exclusions, insurers must consider two other issues to determine whether there is in fact a claim for "personal and advertising injury." The first concerns whether there was a claim for violation of privacy asserted in the underlying litigation. Under the relevant definition of "personal and advertising injury," to obtain coverage for a data breach-type event, the alleged injury must violate a "person's right of privacy." When a complaint does not specifically make a claim for "invasion of privacy," there may not be coverage for the underlying claims under the law of some jurisdictions. *See, e.g.*, *Maryland Cas. Co. v. Express Prods., Inc.*, Civ. A. No. 08-2909, 09-857, 2011 WL 4402275, at *16 (E.D. Pa. Sept. 22, 2011) (rejecting claim for coverage for "junk fax" allegations, concluding that coverage extends only to secrecy interests). However, Minnesota law does not have that requirement. *Owners Ins. Co. v. European Auto Works, Inc.*, 695 F.3d 814, 820 (8th Cir. 2012) (concluding that coverage can extend to seclusion-based torts that involve intruding on another's solitude, as well as secrecy-based torts such as those directed at disclosure of information).

The most widely litigated issue under Coverage B claims, though, has to do with the question of whether a data breach constitutes "publication." In general, some courts have held that for publication to exist, the information in question must be distributed widely. *See, e.g., Penzer v. Transp. Ins. Co.*, 29 So. 3d 1000, 1005–06 (Fla. 2010). Other courts have allowed claims to proceed when the information is shared with a more restricted group of people in at least some situations. *See, e.g., LensCrafters, Inc. v. Liberty Mut. Fire Ins. Co.*, No. C 04-1001, 2005 WL 146896, at *10 (N.D. Cal. Jan. 20, 2005).

Data breach cases present unique issues in terms of publication. The claims usually involve the theft of personal information from an insured. For example, *In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*, No. 12-347, 2014 WL 1858458 (D.D.C. May 9, 2014), while not an insurance matter, presents a unique fact pattern and lesson on publication. There, an unidentified person broke into a car and stole items, including data tapes with personal information of 4.7 million members of the U.S. military and their families. The tapes were only able to be read on specific hardware and software, however. The court noted that there was no evidence that the thief was able to read the personal information, so there was no evidence of publication to a third party. As a result, the plaintiffs did not have standing to bring their claims.

Where there is no question about whether a third party who stole personal information can view that information, courts have reached different conclusions regarding the question of whether the theft itself constitutes publication. In a case alleging theft, use, and possible sale of personal information, an Ohio court found support for the claim that publication took place. *Galaria v. Nationwide Mut. Ins. Co.*, 998 F. Supp. 2d 646, 658 (S.D. Ohio 2014). However, other courts have reached the opposite conclusion. *See, e.g.*, *Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 83 A.3d 664, 672 (Conn. App. Ct. 2014) ("The plaintiffs have failed to cite any evidence that the information was published and thereby failed to take their allegation beyond the realm of speculation."); *Burton v. MAPCO Exp., Inc.*, 47 F. Supp. 3d 1279, 1288 (N.D. Ala. 2014) ("Mr. Burton offers no legal basis for his claim that a theft of data from a merchant constitutes communication of the information stolen to the public. Without such disclosure to the public at large, there is no tort.").

In 2014, a New York state court issued a widely-watched decision on the issue of publication. That case, *Zurich American Insurance Co. v. Sony Corp. of America*, involved a question of coverage for claims related to the well-publicized breach of Sony's PlayStation network. In that case,

the insurer argued that Coverage B for personal and advertising injury applied to the purposeful and intentional acts of the insured, not to acts by third parties. Sony, the insured, argued that there was no need for an affirmative act, and that its "act" was the alleged failure to properly secure its customers' information. The judge ruled from the bench, finding that there was a publication, but that coverage only applied to the extent that Sony, not the hackers, was responsible for the publication. In his remarks, the judge said that there was no way he could find that Sony perpetrated the publication because Sony had tried to maintain security and the security was breached by the hackers. The case was an important win for insurers, and all awaited the appellate court's decision as it would have been the first to address the issue of whether "publication" requires an affirmative act by the insured, or can be met based on an insured's negligence. A couple months after oral argument before the New York appellate court, though, the parties settled.

CAVEAT

As with Coverage A, CGL policies are beginning to change terms to prevent claims based on the theft of electronic data. A 2013 endorsement to the standard ISO form removes coverage for publication of material that violates a person's right of privacy from the definition of "personal and advertising injury" under Coverage B. That change, and other similar changes, will likely limit, if not eliminate, claims by insureds under their CGL policies for data breaches.

2. Directors and Officers Liability Policies

While claims citing CGL policies are the most common, insureds may seek third-party coverage for defense and indemnification in data breach suits under other insurance coverage. Directors and Officers Liability (D&O) policies provide coverage for alleged wrongful acts of a director or officer of a company/corporation. The coverage usually applies to the decisions and actions of those individuals when taken within the scope of their regular duties. Policies apply to the personal liability of those individuals, as well as reimbursement to the insured company in case it has paid the claim of a third party on a director's or officer's behalf. If purchased, there may also be direct coverage for the company as well. The different insuring agreements for D&O coverage are discussed more at Chapter 23, Directors and Officers Liability Insurance.

Where an underlying claim asserts that the wrongful acts of corporate representatives, including errors, misstatements, omissions, and neglect, caused an injury to a third party, D&O coverage may be implicated. The policies are most often triggered when shareholders file complaints. For example, in light of their highly publicized data breaches, shareholders of Target and Sony, respectively, brought claims against the directors and officers of the companies, alleging that managers failed to implement internal controls to protect personal information, and that such failures breached a fiduciary duty owed to investors. While claims of that nature may prove difficult to establish, *see, e.g.*, *Palkon v. Holmes*, Civ. A. No. 2.14-CV-01234, 2014 WL 5341880 (D.N.J. Oct. 20, 2014), costs to defend (and perhaps indemnify if necessary) may be covered under D&O policies.

Of note, such policies may contain relevant exclusions, including exclusion of coverage for a loss arising out of "services through the transmission of data to or from an Internet website." *Bank of Rhode Island v. Progressive Cas. Ins. Co.*, C.A. No. 13-164-M, 2014 WL 1931906 (D.R.I. May 15, 2014).

PRACTICE TIP

As D&O policies are not as standardized as CGL policies, it is important for an insured to familiarize itself with the particular coverage afforded by its policy.

3. Errors and Omissions Policies

Coverage under an errors and omissions (E&O) policy would be similar to coverage under a D&O policy. E&O policies offer coverage for negligent actions while performing professional services. There has been little coverage litigation on whether E&O policies provide coverage for data breach claims. However, many insurers specifically include exclusions stating that the insurance does not cover the failure to protect personally identifiable information in the care, custody, or control of the insured.

§ 26.3 CYBER LIABILITY INSURANCE

A. Overview of Cyber Liability Insurance

Given the potential gaps in using traditional insurance policies, such as CGL policies, to manage the risk of cyber liability claims, many insureds are looking to specialized cyber insurance products. One consequence of cyber insurance's infancy, though, is the absence of standardized policies or interpretative case law policies. Moreover, the lack of uniformity of cyber policies makes the little case law that does exist of limited value. A practitioner's best tool is to look to the overall purpose of the insuring agreement and the construction of analogous language in other types of policies.

There are six main types of cyber insurance: (1) privacy and crisis management, (2) computer program and electronic data restoration expenses, (3) network business interruption, (4) cyber extortion, (5) network security liability, and (6) enterprise and Internet media. Each type of coverage allows the insured to recover for different types of losses resulting from data breaches.

B. Common Issues

Although different types of cyber insurance cover different causes of loss and expenses, there are issues common to the different types. These issues include the applicability of coverage to data hosted by third parties and to what extent a computer or electronic device must be implicated in the loss.

1. "Computer System"

Most cyber coverage protects insureds from losses related to a "computer system." Accordingly, coverage frequently turns on the definition of "computer system." "Computer system" nearly always includes the insured's own IT infrastructure. The more difficult issue is whether the insurance applies to breaches of vendor or cloud-based systems. Policies that narrowly define "computer system" may not cover data stored on third-party systems.

The coverage analysis of course depends on the facts. For example, some policies require that the insured operate the computer system, whether leased or owned. *See, e.g.*, *Hudson United Bank v. Progressive Cas. Ins.*, 152 F. Supp. 2d 751 (E.D. Pa. 2001). In *Hudson United Bank*, the court interpreted the above language to include a computer system operated on the insured's behalf. The court noted that the computer system was designed to serve the insured's interest and that a third party operated the system on behalf of the insured. The court also noted that the third party's computer system transmitted information directly to the insured's system. The court concluded that, although the network was operated by a third party, because it was operated on the insured's behalf, the arrangement satisfied the requirement that the insured operate the system.

Some policies include a broader definition of "computer system," which expressly incorporates computers used on behalf of the insured. *See, e.g.*, *First Bank of Del. v. Fid. & Deposit Co. of Md.*, C.A. No. N11C–08–221, 2013 WL 5858794, at *3–4 (Del. Super. Ct. Oct. 30, 2013) ("[The policy] defines a 'Computer System' as … related communication networks including the internet, used by the Company or used to transact business on behalf of the Company.") To fall under this definition of "computer system," the system need not be used primarily to benefit the insured. It may be that a third party also benefits from the arrangement. For example, in *First Bank of Delaware*, the insured had a relationship with a third party that allowed the insured to use the third party's computer system to transfer money between financial institutions. The third party also benefited because it was able to access the credit card company's networks with the insured's credentials. Although the court acknowledged that multiple parties benefited from the arrangement, the court concluded that the system was within the policy's definition of "computer system." *Id.* at *5–6.

Depending, of course, on the particular language of the policy, case law on property insurance suggests that Minnesota courts may also adopt a broader interpretation of "computer system." As Minnesota courts have stated, "it is not necessary that the insured should have an absolute right of property" in damaged property for coverage to apply. *Nw. Nat'l Bank of Minneapolis v. Maher*, 258 N.W.2d 623, 625 (Minn. 1977) (quoting *Banner Laundry Co. v. Great E. Cas. Co.*, 180 N.W. 997, 999 (Minn. 1921)). In *Maher*, the court concluded that coverage applies to the property if "by the destruction of the property, [the insured] will suffer a loss, whether [the insured] has or has not any title to, lien upon or possession of the property itself." *Id.* Therefore, it seems likely that when the question arises, a Minnesota court will hold that an insured need not have an exclusive, possessory interest in a computer system to obtain coverage under a policy.

Not all policies require that the loss result from the use of a computer. Some cyber policies allow for recovery of losses that result simply from the loss of confidential information. One example of such a policy reads: "The Insurer shall pay on an Insured's behalf all Loss in excess of the applicable Retention that such Insured is legally obligated to pay resulting from a Claim alleging a Security Failure or a Privacy Event." AIG, *Specialty Risk Protector ®: CyberEdge Security and Privacy Liability Insurance*, *available at* <www.aig.com/Chartis/internet/US/en/SECURITY%20AND%20PRIVACY%20COVERAGE%20SECTION%20101024%20(12-13)%20SRP%20Coverage%20Parts_tcm3171-661710.pdf>. (bolding of defined terms omitted). Such policies often define "privacy event" broadly to include "any failure to protect Confidential Information … including, without limitation, that which could result in an identity theft." *Id.* at 4. Under this broad definition, a "privacy event" may include physical data breaches. For example, coverage may apply to losses resulting from the loss or theft of an employee's computer that contains confidential information.

NOTE

A strong cyber and privacy policy will not even require that the confidential information be electronically stored; depending on the circumstances, the policy quoted above may afford coverage for damages that arise out of the loss or theft of a briefcase containing hard copy confidential information.

2. Cause of Loss

A similar issue arises over how close the causal connection must be between the loss and the use of the "computer system." Construing language in a fidelity bond, one Minnesota court concluded that coverage applies if the data breach is a foreseeable and natural consequence of the computer use. *State Bank of Bellingham v. BancInsure, Inc.*, No. 13–cv–0900, 2014 WL 4829184, at *21 (D. Minn. Sept. 29, 2014). The court's conclusion stemmed from Minnesota's common law rule that for coverage to apply, a covered cause of loss must be "the efficient and proximate cause" of the loss. An excluded peril will only bar coverage if it is the "overriding cause" of loss. Stated another way, only if the loss is the foreseeable and natural consequence of the excluded peril will coverage be precluded. *Id.*

BancInsure demonstrates how this rule could be applied in the cyber insurance context. In *BancInsure*, the insured was defrauded out of nearly $500,000 after a computer hacker installed a virus on the insured's computer. The virus allowed the hacker to initiate unauthorized financial transactions from the insured's computer network. The insured filed a claim on a bond issued by the insurer. The insuring agreement provided coverage for a "[l]oss resulting directly from a fraudulent … entry of Electronic Data or Computer Program into … any Computer System operated by the Insured." The insurer argued that the exclusion for losses caused by an employee applied. As the proximate cause of the loss, the insurer pointed to the employee's downloading of a virus from an email, failing to update antivirus software, and failing to follow computer security protocols. The court disagreed, concluding that the employee's conduct was not the efficient proximate cause of the loss. The court reasoned that but for the hacker's fraudulent conduct, the money would not have been transferred. Therefore, a hacker's fraudulent wire transfers were not a foreseeable and natural consequence of the employee's failures. The court summarized its reasoning, stating that "without the fraudster's actions, there would have been no loss even if all of the other circumstances existed." *Id.* A Connecticut Superior Court adopted similar reasoning in *Owens, Schine & Nicola v. Travelers Casualty & Surety Co. of America*, No. CV095024601, 2010 WL 4226958, at *6 (Conn. Super. Ct. Sept. 20, 2010) ("The emails were the proximate cause and 'efficient cause' of [the insured's] loss because the emails set the chain of events in motion that led to the entire loss."). *But see Brightpoint Inc. v. Zurich Am. Ins. Co.*, No. 1:04-CV-2085-SEB-JPG, 2006 WL 693377, at *7 (S.D. Ind. Mar. 10, 2006) (concluding that the electronic receipt of a fraudulent purchase order did not trigger coverage because the purchase order only notified the insured of the purchase, and the insured did not execute the sale until it received checks and bank guarantees).

PRACTICE TIP

There are similarities between the analysis of the terms "cause of loss" under cyber insurance policies and "use of a computer" under the more traditional crime insurance policies. Courts examining these newer policies may find case law addressing the "use of a computer" to be persuasive in analyzing the "cause of loss."

C. Specific Types of Cyber Liability Policies/Coverage

Turning then to specific types of cyber insurance coverage, the six most common categories of coverage in the market today are (1) privacy and crisis management, (2) computer program and electronic data restoration expenses, (3) network business interruption, (4) cyber extortion, (5) network security liability, and (6) enterprise and Internet media. The first four are typically thought of as first-party type coverage, while the final two are more akin to third-party type coverage. Note that these coverages could be presented as stand alone policies, or could be different types of coverages within an overall insurance package. Moreover, the various insurers may use different terms to describe these types of coverage. The terms referenced herein are descriptive, and these types of coverages, no matter what the name used by the insurer, usually contain common coverage features such as those discussed below.

1. Privacy and Crisis Management Coverage

Privacy and crisis management cyber insurance is first-party insurance that covers the immediate costs of responding to a data breach. The activities covered by privacy and crisis management coverage are ones that help the insured mitigate damages and avoid liability resulting from the breach. As discussed in the overview section, costs associated with a data breach can be high. Consequently, insureds concerned about this type of risk should consider a higher limit for such policies. The benefit to this type of coverage is that the scope of liability is likely to be known or at least estimable.

EXAMPLE

A typical insuring clause for a privacy and crisis management policy provides:

The Insurer shall pay all Loss, in excess of the applicable retention, less the applicable Coinsurance percentage that an Insured incurs solely as a result of an alleged Security Failure or Privacy Event that has actually occurred or is reasonably believed by such Insured and the Insurer to have occurred.

While this insuring agreement is not clear on the type of coverage at issue, the definition of "loss" makes clear that it is a privacy and crisis management type policy. The definition of "loss" in a strong privacy and crisis management policy will include expenses for (1) conducting an investigation to determine the cause of the breach; (2) hiring a public relations, crisis management, or law firm; (3) notifying affected individuals; (4) monitoring affected individuals' credit; and (5) restoring or recreating lost data.

NOTE

Privacy and crisis management coverage may include sublimits for each of the types of expenses it covers. The sublimits may be written as a threshold based on the number of records affected.

In selecting privacy and crisis management coverage, insureds should be mindful about how the public relations firm will be selected and how notification will be handled. In some instances, the insurer may handle notification expenses. Although insureds may be reluctant to cede control of this process, insurers often have experience with the notification process. Insurers may also want to handle notification costs because they have negotiated rates with vendors who handle notification. Of course, depending on the importance of such matters to the insureds, that may be a negotiable point.

PRACTICE TIP

Policies may also place limits on the selection of a public relations firm. Some policies will allow the insured to select the public relations firm, while others will require that the client select from panel firms approved by the insurer. Again, as with many of these types of issues (akin to selection of counsel versus panel counsel), it may be a negotiable point with the insurer.

2. Computer Program and Electronic Data Restoration Expenses

Insureds may need to purchase coverage for data restoration separately from the insureds' primary first-party cyber insurance policy. Data restoration coverage should cover the cost of restoring both data and computer programs.

EXAMPLE

The following is an example of a data restoration insuring agreement:

The Insurer will pay the Insured for Restoration Expenses incurred by the Insured that are directly incurred by the Insured which are directly caused by a Computer Violation taking place prior to the expiration of the Policy Period and Discovered during the Policy Period.

Restoration expenses should include expenses to replace or reproduce damaged or destroyed computer programs or electronic data. The policy should cover data and programs stored within a "computer system" owned or leased by the insured, or operated on the insured's behalf. Note, though, that if the insured determines that the computer program or data cannot be restored or replaced, the policy may only cover costs of making that determination. Thus, the policy would not pay for the value of lost data that cannot be restored. Note too that both the loss of the data and the discovery of the loss must take place during the policy period. Consequently, coverage may not be available if the insured discovers that data was lost after coverage has lapsed, even if the loss of data occurred during the coverage period. Such a situation may arise with programs or data that are used intermittently.

There are several important exclusions for this type of coverage. First, coverage may be excluded for data or computer programs destroyed by computer software the insured did not have license to use. Second, insureds may not be able to rely on this coverage to "design, update, improve, or perfect the operation of or performance of computer programs."

Difficult issues may arise under both of these exclusions. For example, if an employee illegally downloads protected software and the software contains a computer virus, will the first exclusion preclude coverage? Similarly, under the second exclusion, if a computer virus does not destroy a computer program, but causes the program to operate more slowly, will restoration coverage apply? These issues may be resolved by looking to the definition of "computer violation" (or similar terminology), which must cause the data loss. "Computer violation" should include a network's infection with a virus or the unauthorized access of a computer system or access by an authorized user for wrongful means.

As to the first issue—illegal downloading of software by an employee—if either a computer virus or unauthorized access leads to loss or impairment of data, the event is arguably covered, and unauthorized use by an employee should not negate coverage. Depending on the circumstances, the insured may have a reasonable expectations argument. *See, e.g.*, *Atwater Creamery v. W. Nat'l Mut. Ins.*, 366 N.W.2d 271 (Minn. 1985). As for the second issue—a computer virus that simply slows down a program—even if data or a computer program is not totally destroyed, coverage may be available if the use or function of the data or program are impaired. *Cf. Sentinel Mgmt. Co. v. N.H. Ins.*, 563 N.W.2d 296, 300 (Minn. Ct. App. 1997) (concluding that the release of asbestos into a building is covered under a property insurance policy because the building's function or use was impaired). The argument for coverage will be even stronger if the policy expressly includes coverage for both destroyed and damaged data.

3. Network Business Interruption Coverage

A third type of cyber insurance is network business interruption coverage. This type of cyber insurance is a first-party policy similar to traditional property insurance. Network business interruption coverage provides coverage to the insured for loss of income and extra expenses due to interruption of an insured's business caused by a network security failure.

The insuring language in a typical network business interruption policy states: "The Insurer shall pay all Loss in excess of the Remaining Retention that an Insured incurs after the Waiting Hours Period and solely as a result of a Security Failure." The cause of interruption (the "security failure") is important to whether network business interruption coverage will respond to the loss. Network business interruption coverage generally will only apply if the interruption is caused by a failure or compromise of the security of a computer system. Examples of such a failure include unauthorized access to the insured's system or the transmission of malicious code that destroys computer files. In contrast, if a fire causes the insured's network to fail, the insured should look to its property insurance for coverage.

Note, though, that some policies go beyond *security* failures and cover *system* failures. Coverage for a system failure will cover losses resulting from an accidental outage.

Network business interruption coverage will only apply to security failures on a "computer system." But, as discussed above, which computer systems fall within this definition varies. See discussion at section 26.3.B.1, *supra*.

Minnesota appellate courts have not explored the contours of network business interruption coverage. Fortunately, network business interruption coverage is similar to traditional contingent business interruption coverage, which Minnesota courts have analyzed. Many of these decisions should be applicable to the cyber insurance context.

"The purpose of coverage for business interruption loss is to do for the business what it would have done for itself had no loss occurred." *Wood Goods Galore v. Reinsurance Ass'n of Minn.*, 478 N.W.2d 205, 209–10 (Minn. Ct. App. 1991). Business interruption expenses are calculated based on the loss of gross earnings minus expenses saved due to the business's discontinuance. *Metalmasters of Minneapolis v. Liberty Mut. Ins.*, 461 N.W.2d 496, 500 (Minn. Ct. App. 1990). These expenses should include expenses incurred to restore the computer network to the extent restoring the network is necessary to mitigate business interruption losses. *See id.* at 501 ("If … the insured has a contractual as well as a common law duty to mitigate damages, then the expenses of that mitigation must be covered."). In some cases, insureds may receive compensation for mitigation expenses incurred after normal business operations resume. *Id.* ("If the mitigation efforts take longer than the interruption period, then the business interruption clause cannot limit coverage to that period, since the activity is in the interest of the insurer."). These mitigation expenses must, however, be reasonable and less than what the damages would have been without the mitigation. *Id.*

Network business interruption coverage will frequently include a cut off date. "A 'cut off' date is a necessity. Otherwise, claims would be open to a degree of speculation which would be absurd." *Great N. Oil v. St. Paul Fire & Marine Ins.*, 227 N.W.2d 789, 793 (Minn. 1975) (quoting *Rogers v. Am. Ins.*, 338 F.2d 240, 243 (8th Cir. 1964)). This cut off date prevents the insured from recovering for losses incurred after a certain number of days since normal business operations resumed.

As its name suggests, network business interruption coverage should apply to material or measurable interruptions in business, not simply to total suspensions in business operations. *See Archer Daniels Midland Co. v. Aon Risk Servs. of Minn.*, 356 F.3d 850, 856 (8th Cir. 2004) (concluding that coverage was not limited to expenses "incurred as a result of a complete cessation of business"). *But see Forestview The Beautiful, Inc. v. All Nation Ins. Co.*, 704 N.W.2d 773, 776 (Minn. Ct. App. 2005) (concluding that the plain meaning of "suspension" in the insured's policy did not include a partial suspension of business operations).

Network business interruption coverage will frequently include a waiting period. These waiting periods operate much like deductibles, allowing insurers to avoid indemnifying insureds for frequent, nominal business interruptions. The insured will not be able to recover for business interruption losses that arise during this waiting period. Waiting periods range from hours to days.

PRACTICE TIP

For some insureds (depending on their business), mere hours down after a security or system failure can be disastrous, whereas other insureds can shoulder a longer period of suspension. Moreover, warranty and indemnification obligations by a third-party vendor may kick in at a much shorter period of time, thereby potentially reducing the value of the business interruption coverage. As such, the waiting period is a term to which the insured should pay particular attention.

4. Cyber Extortion Coverage

Cyber extortion coverage has a narrow application, but one that is becoming increasingly common. Cyber extortion is one the fastest growing forms of computer hacking. Joyce M. Rosenberg, *Pay a Ransom or Lose Your Files – Hackers Force Computer Users to Make a Hard Choice*, STAR TRIBUNE, Apr. 8, 2015, *available at* <www.startribune.com/lifestyle/299063761.html>. Cyber extortion occurs when an outsider threatens to release, disseminate, destroy, block access to, or steal confidential information. The perpetrator will often do so through "ransomware." *Id.* Cyber extortion coverage should pay both ransom and expenses incurred in investigating the demand.

EXAMPLE

Insuring language for cyber extortion coverage may read:

"The Insurer shall pay all Loss in excess of the applicable Retention that an Insured incurs solely as a result of a Security Threat." "Security threat" may be defined as:

> Any threat or connected series of threats to commit an intentional attack against a Computer System for the purpose of demanding money, securities or other tangible or intangible property of value from an Insured.

Some policies may require that the insurer provide its written consent before ransom is paid. The policy may also require that a third-party consultant recommend that the insured pay the ransom. Courts are likely to give effect to this language.

CAVEAT

Insureds should be wary of consent restrictions because the time necessary to obtain the consent or consultant's recommendation may be costly for the insured who, in the meantime, may not have access to its network.

Disputes may also arise over what constitutes cyber extortion. For example, companies with a preexisting relationship may use threats to deny access to data to coerce repayment of a debt. Take the following examples: An insured may receive technology services from a vendor. If the relationship sours, the vendor may prevent the insured from fully utilizing the insured's network until an alleged

debt is paid. Alternatively, the technology company could be the insured and install proprietary software on a client's computer. If the relationship deteriorates, the client may deny the insured access to the company's computers and, as a result, a means of removing the proprietary software. *See, e.g.*, *United Westlabs v. Greenwhich Ins. Co.*, C.A. No. 09C–12–048, 2011 WL 2623932 (Del. Super. Ct. June 13, 2011). In such circumstances, an insurer may take the position that this type of dispute is not the type of dispute cyber extortion insurance was intended to cover. The argument may be persuasive under a definition of "security threat" such as the above, which requires an "intentional attack." However, the *United States* court found "no substantive distinction between threats to cut off service for failure to pay fees and 'cyber extortion.'" *Id.* at *11.

PRACTICE TIP

Cyber extortion coverage may already be part of an insured's existing kidnap/ransom coverage, which is often part of a crime policy. It is important to study the precise contours of such coverage before concluding it is sufficient to cover an insured's risks.

5. Network Security Liability Coverage

Network security liability coverage is the principal form of third-party cyber insurance. Network security liability coverage provides coverage for liability to others resulting from the insured's failure to protect, manage, or store personally identifiable information or corporate information subject to a non-disclosure agreement. Network security liability insurance, when triggered, covers the costs of legal counsel to defend against lawsuits. These lawsuits may come from customers whose confidential information was compromised. Liability may also stem from financial institutions whose customers' data were exposed. Additionally, shareholders might bring a derivative action against the insured. Finally, the insured may be liable for government-imposed fines. Network security liability policies are designed to cover some, if not all, of these expenses. Unfortunately, because exposure for expenses covered under network security liability insurance depends on how third parties respond to data breaches, it is difficult to predict the potential liability (and, therefore, the appropriate limits) for these types of claims.

EXAMPLE

An insuring clause for a network security liability policy may read:

The Insurer shall pay on the Insured's behalf all Loss in excess of the applicable Retention that the Insured is legally obligated to pay resulting from a Claim alleging a Security or a Privacy Event.

A strong cyber liability insurance policy should respond not only to claims brought by private parties but also to suits brought by government agencies. Moreover, the definition of "security failure" in a strong policy will include (at least): (1) failure or violation of the security of a computer system, (2) physical theft of hardware controlled by the insured, and (3) failure to disclose such events in accordance with a notification law. A policy may even respond broadly to claims resulting from the theft of confidential information in any form (including hard copy documents).

Many issues that arise under traditional third-party liability policies are applicable to network security liability policies. Although Minnesota courts have not addressed the duty to defend under network security liability policies, there is no principled basis for distinguishing between the duty to defend under a cyber liability policy and traditional liability policies. Therefore, as with other liability insurance policies, the duty to defend under a cyber liability policy is likely broader than the duty to indemnify. *See, e.g.*, *Brown v. State Auto. & Cas. Underwriters*, 293 N.W.2d 822, 825 (Minn. 1980). The duty to defend arises if any part of the claim is arguably within the scope of indemnity coverage. *Id.* The complaint typically controls whether the insurer has the duty to defend. *See, e.g.*, *Garvis v. Emps. Mut. Cas.*, 497 N.W.2d 254, 256 (Minn. 1993). If the insured provides facts showing arguable coverage, the insurer must satisfy the heavy burden of proving that no duty to defend exists. *See In re Liquidation of Excalibur Ins. Co.*, 519 N.W.2d 494, 497 (Minn. Ct. App. 1994). Once the duty to defend is triggered, generally speaking (depending on the wording of the policy) the insurer has the right to select counsel. *See Mut. Serv. Cas. Ins. Co. v. Luetmer*, 474 N.W.2d 365, 368 (Minn. Ct. App. 1991). Chapter 6, Duty to Defend, discusses the duty to defend in greater detail.

Most network security liability policies are written on a claims-made basis. Under a claims-made policy, a *claim* for a data breach (rather than an *occurrence* of damage from a data breach) that arises during the policy period may be covered, even if the data breach/incident occurred before the policy period. To determine how far back before the policy period the data breach/incident can occur and still be covered (assuming the claim is made during the policy period), the insured needs to determine if the policy includes a retroactive date. If the policy does not mention a retroactive date, then it should not matter when the data breach/incident occurred; the only relevant issue will be whether the claim was made during the policy period. If the policy includes a retroactive date, then not only must the claim be made during the policy period, but the data breach or relevant incident must have occurred after the retroactive date. *See, e.g.*, *In re Silicone Implant Litig.*, 667 N.W.2d 405, 409 (Minn. 2003).

PRACTICE TIP

Insureds who purchase claims-made cyber liability policies should consider, if possible, purchasing a policy with no retroactive date, or with a retroactive date that permits coverage for claims made during the policy period that relate to incidences that occur for some period of time before the policy period.

NOTE

If the policy or coverage is the first cyber liability coverage the insured is purchasing, the default will likely be that the retroactive date coincides with the effective date of the first policy period. In other words, the policy will not provide coverage for a data breach/incident that occurs prior to the policy period.

Conversely, claims may arise after the policy period for breaches or injuries that arose during the policy period. If the insured continues to purchase claims-made cyber liability coverage in subsequent years, such a claim likely would fall under the subsequent insurance policy. However,

if the insured for some reason decides not to purchase a subsequent policy, or is otherwise concerned about a gap in coverage, many cyber liability policies allow the insured to elect to purchase an extended reporting period. An extended reporting endorsement lengthens the amount of time in which an insured may report a claim. *See, e.g.*, *St. Luke's Hosp. of Duluth v. Minn. Joint Underwriting Ass'n*, No. A09-2035, 2010 WL 2733326, at *3 (Minn. Ct. App. July 13, 2010). The claim must still relate to an incident that arose during the policy period, however. These endorsements do not change the type of coverage provided, or provide additional limits of liability.

While not common, it is possible that network security liability coverage could be written on an occurrence basis (so that the date of occurrence rather than the date of the claim is the important consideration). Policies written on an occurrence basis raise different issues. For example, issues may arise under network security liability coverage as to whether an occurrence arose during the policy period. The issue may arise with network security liability because data breaches are frequently detected long after the breach occurs (often almost a year after the breach). Under occurrence-based policies, to determine when the occurrence happened, Minnesota courts use the injury-in-fact or actual-injury rule. *See In re Silicone Implant Litig.*, 667 N.W.2d at 415. Under this rule, the triggering event is not the wrongful act but the damage. Coverage is triggered if the *injury* occurred during the policy period. The insured need only show that some damage occurred during the policy period.

If the policy is written on an occurrence basis, the injury-in-fact rule raises the issue of which policy year should respond to the claim. For example, an unauthorized user may access a computer and install malicious software that lays dormant for a period of time. If, in its dormant state, the malicious software does not injure the claimants during the policy period, coverage is unlikely to be triggered. That the dormant software arguably injures the insured's own computer network is immaterial for *third-party* coverage; only the claimant's injury is relevant.

The more difficult question is whether occurrence-based cyber liability insurance would respond to the mere exposure of the claimants' data to an unauthorized user. For example, if the claimants' data were stolen during the policy period, but the claimants did not suffer financial or other harm at all or at least until after the policy period, will there be coverage for the claim? Such a claim may trigger the broader duty to defend (depending on the broad nature of the allegations of the complaint). Ultimately, though, the duty to indemnify may never be triggered because of a lack of injury. If courts apply the same injury-in-fact rule that they apply in standing cases, the mere increased risk of identity theft as the result of a data breach may not trigger coverage under occurrence-based policies. *See, e.g.*, *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011) (holding that increased risk of future identify theft as the result of a data breach does not satisfy the injury-in-fact rule necessary to satisfy standing requirements); *In re Science Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14 (D.D.C. 2014) (same); *see also, e.g.*, *In re Target Corp. Customer Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) (permitting lawsuit by customers affected by Target's data breach to proceed beyond motion to dismiss, based on some allegations that plaintiffs suffered "unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees," even though not all had alleged *unreimbursed* injury, but noting that Target could raise the issue again on summary judgment following discovery); *U.S. Hotel & Resort Mgmt. v. Onity, Inc.*, Civ. No. 13–1499, 2014 WL 3748639, at *5 (D. Minn. June 30, 2014) (observing that majority of courts hold that plaintiffs "whose confidential data has been exposed, or possibly exposed, by theft or a breach of

an inadequate computer security system, but who have not yet had their identity stolen or their data otherwise actually abused" do not satisfy the injury-in-fact requirement).

The contractual liability exclusion is one to be aware of in cyber liability policies, whether written on an occurrence or a claims-made basis. Many insureds will obtain data from sophisticated third parties that require the insured to indemnify the third party for liability for damages the third party incurs as a result of the insured's handling of the data. Conversely, many cyber liability policies include an exclusion for damages by reason of the assumption of liability in a contract or agreement. This type of exclusion is similar to contractual liability exclusion found in CGL policies.

Like CGL policies, cyber liability contractual liability exclusions may include exceptions for liability that would arise in absence of the agreement or for a contract or agreement that is an "insured contract." Moreover, note that Minnesota courts have taken a narrow view of the contractual liability exclusion in CGL policies, concluding that the exclusion merely excludes coverage if the insured "gratuitously undertakes to act as surety or … undertakes contractual obligations not arising as a matter of law in the conduct of its business." *Sphere Drake Ins. Co. v. Tremco, Inc.*, 513 N.W.2d 473, 481 (Minn. Ct. App. 1994). Thus, assuming a court applies this narrow construction of a contractual liability exclusion to a similar exclusion in a cyber liability policy, the exclusion likely would be inapplicable to many claims, as the insured generally will only collect third-party data as part of a reciprocal business relationship (rather than "gratuitously acting as a surety for the third party's loses"). However, it is important to acknowledge that the presence of such an exclusion on the policy will likely trigger a dispute as to coverage.

It is also important to note that the contractual liability exclusion does not apply to liabilities that arise under statute. *See, e.g.*, *Auto-Owners Ins. Co. v. Newmech Cos. Inc.*, 678 N.W.2d 477, 483 (Minn. Ct. App. 2004). Thus, the increased number of statutes that impose liability on those who mishandle others' data may further circumscribe the contractual liability exclusion. *See, e.g.*, 42 U.S.C. §§ 1320d–2(d), 1320d (imposing penalties on those who, among other things, breach security standards for protecting patients' health information).

CAVEAT

Insureds need to be aware of any policies that contain exclusions for violation of a statute, rule, or law. Given the continuing expansion of consumer protection laws aimed at addressing data breaches, such an exclusion could severely erode coverage.

PRACTICE TIP

There are other types of exclusions insureds should be wary of. For example, insureds seeking broad network security liability coverage need to ensure that the coverage extends to information in the "care, custody, or control" of the insured's vendors, rather than just the "care, custody, or control" of the insured (so that the insured is not relying solely on the vendor's indemnification obligation and insurance—and perhaps additional insured status—to cover a claim). An insured should also be aware of coverage that is limited to just criminal-type breaches, or policies that

PRACTICE TIP (CONT'D)

exclude coverage for "insider" type breaches, to the exclusion of accidental losses/leaks and breaches caused employees. Insureds should also take note of any encryption requirements (requiring data to be encrypted) that apply before coverage will be triggered; these are often onerous requirements that simply provide a hurdle to coverage.

6. Enterprise and Media Liability Insurance

The final form of the typical types of cyber insurance coverage is enterprise and media liability insurance. Enterprise and media liability insurance is a form of third-party insurance. The insurance provides coverage from liability for advertising injury claims. Advertising injury claims include claims for infringement of others' intellectual property rights and defamation. This coverage may overlap (unless more recent exclusions are part of the insured's CGL policy, *see* discussion at section 23.2.B.1, *supra*) with Coverage B under an insured's CGL policy. Consequently, the terms of the insured's CGL policy should influence whether, and to what extent, the insured purchases media liability coverage.

Media liability coverage's importance only increases as companies continue to expand their use of the Internet and social media to communicate with the public.

EXAMPLE

The following is an example of an insuring agreement for enterprise and media liability insurance:

The Company will pay on behalf of the Insured, Loss for any Claim, other than a Regulatory Claim, first made during the Policy Period or, if exercised, during the Extended Reporting Period or Run-Off Extended Reporting Period, for a Communications and Media Wrongful Act.

The key definition in this insuring agreement is "communications and media wrongful act." The definition should at least include coverage for claims for (1) unauthorized use or infringement of copyright, trademark, trade dress, service mark, etc.; (2) invasion of or interference with a right of privacy; and (3) defamation, libel, slander, etc. Note, though, that enterprise and media liability coverage insurance policies may not cover claims based on false advertising. *See, e.g.*, *Sony Computer Entm't Am. Inc. v. Am. Home Assurance Co.*, 532 F.3d 1007, 1016–18 (9th Cir. 2008); AIG, *Specialty Risk Protector* ®: *CyberEdge Security and Privacy Liability Insurance*, *available at* <www.aig.com/Chartis/internet/US/en/MEDIA%20CONTENT%20COVERAGE%20SECTION%20(CLAIMS%20MADE)%20101019%20(12-13)%20SRP%20Coverage%20Parts_tcm3171-661703.pdf>.

A narrow policy will only include content displayed or distributed by the insured by electronic means. This definition includes infringing material on an insured's website. But a broader policy will also include infringements occurring in printed materials.

There are few court decisions on cyber media liability policies. There are more decisions on traditional media liability policies. These decisions foreshadow issues likely to arise under enterprise

and media liability policies. As noted with respect to the discussion of coverage under Coverage B of traditional CGL policies, one issue that arises under traditional media policies is how wide the information must be distributed for any resulting claim to fall within the scope of coverage. *See* discussion at section 26.2.B.1.b, *supra*; *see also Liberty Mut. Ins. v. Westport Ins.*, 664 F. Supp. 2d 587, 593 (D.S.C. 2009) (finding no coverage in case where a news executive made defamatory statements about a third party to a colleague because the media liability policy required that the allegedly defamatory language come in the form of "words, sounds, or images, made … to a *mass public audience* through the insured's public broadcasts, films or other forms of *mass media*").

Such a coverage issue could arise in the cyber media liability context if an alleged defamatory statement were transmitted to a small number of individuals via email. As in *Westport Insurance*, coverage is likely to turn on the scope of the terms in the insuring agreement. A policy that provides coverage for "media content in any form, including, without limitation, [printed and electronic] content, of: … broadcasts … [or] publications," may be construed to only cover content that is widely distributed because of the qualifier "broadcasts or publications." Alternatively, a policy that covers "any content made known, displayed or disseminated via any electronic means, including websites and electronic mail," with no further qualifier, may cover an email sent to a limited number of individuals.

PRACTICE TIP

Another issue that may come up in media and enterprise coverage is the scope of any breach of contract claim exclusion. A coverage dispute may arise if the insured agrees to license its intellectual property to a third party who eventually sues the insured for violating the terms of the license agreement. Such a situation arose in *General Insurance Co. of America v. Marvel Enterprises*, No. 604690/01, 2002 WL 34357984 (N.Y. Sup. Ct. June 26, 2002). In that case, the insured licensed its characters "X-Men" to a movie studio. The movie studio sued the insured for copyright infringement after the insured began collaborating with a television studio to begin promoting a television series titled "Mutant X." The media liability insurer denied coverage, in part, based on the breach of contract claim exclusion, which negated coverage for "claims … for or arising out of any … actual or alleged breach of any contract, agreement or warranty." The insurer maintained that "but for" the licensing agreement conveying to the movie studio the right to produce an "X-Men" movie, no claim would arise. In a declaratory judgment action brought by the insurer, the court concluded that the breach of contract claim exclusion was not applicable because the movie studio's claims "are independent claims that [the movie studio] could have asserted regardless of any alleged breach of the [licensing agreement]." *Id*. Minnesota courts follow the same "but for" analysis addressed by the court in *Marvel Enterprises*. *See, e.g.*, *Zayed v. Arch Ins. Co.*, 932 F. Supp. 2d 956, 961–62 (D. Minn. 2013) ("Under Minnesota law, the phrase "arising from *x*" encompasses any claim that would not exist 'but for *x*'"); *see also Faber v. Roelofs*, 250 N.W.2d 817, 822 (Minn. 1977). Accordingly, for insurance policies that preclude coverage for liability "arising out of" a breach of contract, coverage may be excluded if the third-party claim would not exist "but for" the contract. *See* AIG, *Specialty Risk Protector*®: *CyberEdge Security and Privacy Liability Insurance*, *available at* <www.aig.com/Chartis/internet/US/en/MEDIA%20CONTENT%20COVERAGE%20SECTION%20(CLAIMS%20MADE)%20101019%20(12-13)%20SRP%20Coverage%20Parts_tcm3171-661703.pdf>.

§ 26.4 CONCLUSION

As the use of the Internet and the collection and dissemination of electronic data has grown, risks have grown. Individuals and businesses rely heavily on computers, collect much information, and share that information electronically. Most people's name, address, Social Security number, credit card information, and bank account information is stored and transmitted in electronic form by one or many companies. Hackers have shown an ability to access that information by breaching the security provisions many companies have put in place. As a result, millions of individuals have had their personal information stolen in one form or another.

Calculating damages in data theft cases has proven to be difficult. However, claims can be significant. Insurance companies were slow to anticipate the risks, and some courts found that coverage existed under traditional policies. As the insurance companies came to understand the potential exposure in a data breach case, they began to change the terms of coverage. While there will likely be some cases involving issues under "traditional" insurance policies of whether a loss involves tangible property or intentional publication by an insured, those cases will become fewer and further between. Endorsements and changes in policy language adopted by the insurance industry will exclude most claims made under such policies. As a result, the industry will likely see a dramatic growth in cyber insurance policies.

The lack of standardization in the cyber insurance industry will lead to some uncertainty about the scope of coverage in the near term, and insureds need to closely scrutinize the risks they are seeking to cover against the coverage terms of the policies. As cyber risks continue to grow, though, it is likely that the courts will be called upon to shed light on the bounds of coverage under cyber insurance policies.