

## PROTECTING YOUR COMPANY AGAINST LOSS OR LIABILITY ARISING FROM CYBERATTACKS

By Scott N. Godes and Kenneth Berline Trotter

Does your company have insurance policies that will cover data breaches and cyber attacks? The hospitality industry is particularly vulnerable to data breaches and other cyberattacks. According to Willis Group Holdings, a British insurance firm, insurance claims for data theft worldwide jumped 56% last year, with a large number of those attacks targeting the hospitality industry. The report said the largest share of cyber attacks—38%—were aimed at hotels, resorts and tour companies. As just one example of these attacks, computer hackers broke into the computer system of a national hotel chain and stole the guests' credit card information. This summer, the Secret Service informed the owner of a family-run Italian restaurant that a thief hacked into the communication system between the cash register and the credit card processing company, stole credit card numbers, and then used them to fraudulently make purchases across the United States. Businesses in the hospitality industry will continue to be attractive targets for hackers and data thieves, particularly since they obtain and maintain confidential data from consumers including countless credit card records. There are risks for companies well beyond the possibility of hackers stealing consumer data. Vital corporate data, whether it's shared on the company's servers or by third parties, may become inaccessible or even destroyed in a hacker attack. Managing such risk is critical to successful business operations.

The financial security and stability of a company depends on more than just the protection of the company's proprietary data and information. The company must also be protected from liability to third parties or the government for data breaches that are difficult to predict, and over which the company often has little control. As one court noted, database breaches "provide the basis for a new breed of lawsuits, and especially class action lawsuits, in which plaintiffs allege . . . that [defendants'] negligence in developing and maintaining security measures have resulted in otherwise personal and confidential information being compromised, thereby increasing the risk of identity theft for those individuals whose information was so compromised." *Amburgy v. Express Scripts, Inc.*, 671 F.Supp.2d 1046, 1050 (E.D. Mo. 2009). Moreover, plaintiffs are starting to have success in asserting that they suffered damages that could be compensable in data breach-related class actions. *See, e.g., Claridge v. RockYou, Inc.*, No. C 09-6032 PJH, 2011 WL 1361588 (N.D. Cal. Apr. 11, 2011). Also, nearly every state has a requirement to report data breaches, in addition to federal laws with reporting requirements.

Since hackers and programmers of malicious software wage a cutting-edge war against those that make more databases and networks secure and reliable, often the best protection a company can get is protection against the consequences of a data breach. Companies may be able to transfer the risks through insurance policies through both new forms of specialty insurance and in traditional forms of insurance. It is important for in-house counsel to work closely with risk managers to understand the insurance policies that the company has or may plan to purchase. That involvement will help protect the company's interests by understanding what insurance coverage will be available to the company for cyber liabilities and data breaches. It also will

help the company tailor its insurance program at the time of policy purchase and renewal.

### **Consider The Insurance That is Available for Your Company to Protect Against Loss or Liability Arising Out of a Cyber Event**

In-house counsel should consult with risk managers, technology managers, and privacy managers to understand the scope of the risks faced by the company. Then, armed with the knowledge of such risks, counsel will be better suited to analyze the appropriate insurance coverage for cyber and data breach risks. When considering what coverages may apply, it is essential to consider virtually all of the insurance policies that a company holds, because the broadly written terms of many “traditional” insurance policies may provide coverage and overlapping coverage for cyber risks and data breaches. Similarly, when purchasing or renewing cyber insurance policies, it is essential to think broadly about a company’s risks and which types of liabilities (from losses as a result of a network being unavailable to potential liability to third parties, for example) the company wishes to ensure, because coverages are often written and offered in different “modules” and on varying insurance policy forms. Insurance companies introduce and revise their cyber insurance and data breach policies frequently, making a careful analysis of the coverages being offered a critical step in an insurance program.

The following policies may be implicated by a cyber event or a data breach. This information should serve as a starting point, and any company facing such risks or liabilities would be well served to engage an experienced broker and outside counsel to assist in evaluating coverage. *Cybersecurity policies* are marketed as providing coverage for cyber risks and data breaches. As these products are new and not as regulated as other insurance policies, the market for cybersecurity policies has been called the “Wild West” of insurance. Cyber security and data breach policies, certain forms of which may be known as Network Risk, Cyber-Liability, Privacy and Security, or Media Liability insurance, are ever-changing. The policies often are sold with various coverage modules, provisions, and insuring agreements. Because of the variety of coverages being offered, a careful review of the policy form and coverages purchased before a claim hits is critical to understand whether the cyberpolicy will provide coverage, and, if it will, how much coverage is available for the event.

*First-Party Property policies* may provide coverage for property damage. Whether such a policy is implicated will typically depend on whether a cyberattack causes physical damage to your company’s servers or hard drives. Even if the damage is limited to data and software, however, it may be argued that the loss is covered under your company’s first-party all risk policy, as some courts have found that damage to data and software consists of property damage. *See, e.g., Lambrecht & Assocs., Inc. v. State Farm Lloyds*, 119 S.W.3d 16 (Tex. App. 2003) (first party property coverage for data damaged because of hacker attack or computer virus); *Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc.*, No. 99-185 TUC ACM, 2000 U.S. Dist. LEXIS 7299, at \*6 (D. Ariz. Apr. 18, 2000) (construing “physical damage” beyond “harm of computer circuitry” to encompass “loss of access, loss of use, and loss of functionality”).

*Business Interruption Coverage* may be purchased as part of a property policy, commercial package policy, or even as stand-alone coverage. Such coverage may reimburse the policyholder for loss due to extra expense, business interruption, and contingent business

interruption losses caused by a cyberattack. (Contingent business interruption losses may include losses that the policyholder faces arising out of a cyber security-based business interruption of another party, such as a cloud provider, network host, or others.) *See Southeast Mental Health Ctr., Inc. v. Pac. Ins. Co.*, 439 F. Supp. 2d 831, 837-39 (W.D. Tenn. 2006) (finding coverage under business interruption policy for computer corruption); *see also* Scott N. Godes, *Ensuring Contingent Business Interruption Coverage*, Law360 (Apr. 8, 2009), <http://insurance.law360.com/articles/94765> (discussing coverage under first party policies resulting from third party interruptions). Courts have considered and found coverage under business interruption and contingent business interruption policies for network interruptions. *See, e.g., WMS Indus., Inc. v. Fed. Ins. Co.*, 588 F. Supp. 2d 730 (S.D. Miss. 2008) (coverage related to interrupted network of gaming machines); *Nat'l Publ'g Co. v. Hartford Fire Ins. Co.*, 949 A.2d 1203 (Conn. 2008) (jury had awarded damages for covered business interruption and extra expense losses resulting from a “computer system [that] did not function properly” because software and databases were stolen).

*Commercial General Liability (“CGL”) policies* may provide coverage for defense costs and judgments or settlements that the policyholder pays because of property damage, (including the loss of use of property), or invasion of privacy claims alleged by customers or other third parties as a result of data breaches or cyber attacks.

The first coverage provided in a standard-form CGL insurance policy covers liability for property damage. Similar to the analysis above for first-party all risk policies, if there was damage to servers or hard drives, insurers are unlikely to argue that there was no property damage. Courts are divided as to whether damage to data or software alone consists of property damage under insurance policies, with some courts recognizing that “the computer data in question ‘was physical, had an actual physical location, occupied space and was capable of being physically damaged and destroyed’” and that such lost data was covered under a CGL policy. *See, e.g., Computer Corner, Inc. v. Fireman’s Fund Ins. Co.*, 46 P.3d 1264, 1266 (N.M. Ct. App. 2002). Be aware, however, that the insurance industry has revised many CGL policies to include definitions giving insurers stronger arguments that damage to data and software will not be considered property damage. But also note that your company’s CGL policy may have endorsements that provide coverage specifically for damage to data and software. *See, e.g., Claire Wilkinson, Is Your Company Prepared for a Data Breach?*, Ins. Info. Inst., at 20 (Mar. 2006), <http://www.iii.org/assets/docs/pdf/informationsecurity.pdf> (discussing the Insurance Services Office, Inc.’s endorsement for “electronic data liability”). Consider further whether a claim would fall within the property damage coverage for loss of use of tangible property—loss of use of servers and hard drives because of the cyberattack; loss of use of computers arising out of alleged software and data-based causes has been held sufficient to trigger a CGL policy’s property damage coverage. *See Eyebaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797 (8th Cir. 2010). Keep in mind that if there is a claim for property damage under a CGL policy, there may be coverage for obligations that your company has under indemnity agreements. Standard form CGL policies provide coverage for indemnity agreements. *See, e.g., Harsco Corp. v. Scottsdale Ins. Co.*, No. 49D12-1001-PL-002227, slip op. (Ind. Super. Ct. Apr. 26, 2011).

Just as significant, if not more so, than property damage coverage, is coverage for personal and advertising injury claims. Such coverage often includes claims relating to the publication of information that was supposed to remain private. Depending upon the allegations of a data breach, the allegations may fall within that coverage. *See, e.g., Netscape Communications Corp. v. Fed. Ins. Co.*, 343 F. App'x 271 (9th Cir. 2009). Note, however, that certain insurance companies have begun to seek court rulings that there is no coverage under personal and advertising coverage for data breaches. *See, e.g., Zurich Am. Ins. Co. v. Sony Corp. of Am.*, No. 651982/2011, complaint (N.Y. Sup. Ct. July 20, 2011).

*Directors and Officers Liability Policies* may provide coverage for investigation costs, *see MBIA, Inc. v. Fed. Ins. Co.*, No. 08 Civ. 4313, 2009 WL 6635307 (S.D.N.Y. Dec. 30, 2009) *affirmed in part and reversed in part by MBIA Inc. v. Fed. Ins. Co.*, 2011 WL 2583080 (2nd Cir. N.Y., July 1, 2011), and *Errors And Omissions Policies* also may provide some coverage, if the cybersecurity claims may be considered to be within the definition of “wrongful act.” *See Eyeblander*, 613 F.3d at 804.

*Crime and Fidelity Policies* may have endorsements, such as computer fraud endorsements, that may cover losses from a denial of service cyberattack. For example, in *Retail Ventures, Inc. v. National Union Fire Insurance Co.*, No. 06-443, slip op. (S.D. Ohio Mar. 30, 2009), the court held that a crime policy provided coverage for a data breach and hacking attack.

### **When Purchasing or Analyzing Coverage, Ask Your Broker Important Cyber-related Questions**

- ✓ Does the company have coverage for first-party claims related to cyber events (*e.g.*, damage to the corporation’s data and property or the interruption of business)?
- ✓ Does the company have coverage for third-party claims related to cyber events (*e.g.*, damages sought from third parties)?
- ✓ Will the insurance policies provide coverage for compliance with state or federal data breach statutes or regulations, even if liability is automatic and self-effectuating, with action required before the government takes action?
- ✓ Will the insurance policies provide coverage for the costs incurred in connection with any governmental investigation or compliance with state regulations for cyber events?
- ✓ Will the insurance policies pay for the following costs that may arise out of a cyber event?
  - The costs of credit monitoring for consumers who have their data misappropriated
  - The costs of defending against potential civil claims
  - The costs of notifying people whose data was potentially exposed
  - The costs arising out of investigations by state attorneys general or other governmental agencies

- ✓ Are there any deductibles, self-insured retentions, or sublimits of coverage that can reduce premiums or the amount of coverage?
- ✓ More specifically, will the policies provide coverage for critical cyber events? (e.g., data breaches; network interruption [from data loss or denial-of-service attacks]; invasion of privacy or a breach of confidentiality; defamation, libel, slander, infringement of copyright, or plagiarism; unauthorized access and hacker attacks [even if made from outside the United States]; cybersecurity claims due to the actions of the company's employees or former employees; failure of IT security or the failure to implement encryption strong enough to prevent attacks; network business interruption and contingent business interruption; restoring, recreating, regaining access to software, data, or other electronic information; theft of a company laptop [on the corporate premises or away from the company's premises]; advertising or remarks made online; alleged violations of copyrights, trademarks, patents, or trade secrets; viruses; spyware; spam; liability arising out of contracts or indemnity agreements; liability arising out of unintentional breach of contract due to alleged improper handling of data or security that could allow for a data breach; and alleged breach of a duty of care)

### **Practical Considerations When Making a Claim for Coverage**

If a cyber event—such as a data breach—occurs, then it is vital that in-house counsel works with its technology managers and privacy managers to understand the scope of the impact to the company and the potential for loss or liability. This will assure that the company can comply with any necessary notice obligations under state regulations and will also help identify all potentially available insurance policies. Companies should send notice of the claim or occurrence to all potentially applicable insurers, whether under a special cybersecurity policy or under the more “traditional” forms of insurance. After an insurance claim is tendered to insurers, they may raise various defenses to coverage; companies, however, should not assume that such defenses will defeat coverage. Whether an event is covered will often depend on careful analysis of the specific policy language involved, the facts of a company's particular losses, and the law of the applicable jurisdiction. Insurance carriers may take a hard line regarding the application of the exclusions in their policies. As previously noted, for example, under certain insurance policies, insurers have asserted that there has been no property damage as a result of a cyberattack and that policies, such as property policies or general liability policies, are not triggered. Working with the company's technology and privacy managers, you may be able to marshal evidence to prove that a cyberattack has damaged the company's computer equipment, or that there has been a loss of use of computer equipment (another way of demonstrating “property damage” under certain insurance policies), and that the company took proper steps to prevent such loss.

### **Conclusion**

With increasing cyber attacks on the hospitality industry, the need for cybersecurity is self-apparent. It is also important to verify that the company will have insurance available for

potential liabilities arising out of any such activities. It is essential that the company receives input from its risk managers, technology managers, privacy managers, and experienced brokers in selecting the right coverage. If a loss or alleged liability has arisen, the company should conduct a complete and thorough analysis of its insurance policies to determine whether insurance coverage is available for the claim. Don't accept the conventional wisdom that there is no insurance available for cybersecurity claims; overlapping coverage may exist in policies that may have been overlooked, even if the company has not purchased express "cyberinsurance." When purchasing coverage, or assessing applicable policies after a loss occurs, it may be prudent to consult with outside counsel who are experienced with cyberinsurance-related issues.

**About the Authors:** Scott Godes and Kenneth Trotter are attorneys with Dickstein Shapiro LLP who devote a significant portion of their practice to the representation of policyholders in complex insurance disputes with their insurance companies; they may be reached at [godes@dicksteinshapiro.com](mailto:godes@dicksteinshapiro.com) or [trotterk@dicksteinshapiro.com](mailto:trotterk@dicksteinshapiro.com). Mr. Godes writes the Corporate Insurance Blog (<http://corporateinsuranceblog.com>), where he often writes about insurance coverage for data breaches, cyber risks, and other claims. He is the national co-leader of the firm's cyber security initiative. Mr. Trotter is the national co-leader of the firm's property and business interruption initiative.