Insurance Recovery for Loss or Liability Arising from Cyberattacks

Obtain and preserve insurance for your company's protection

It is no secret that the hospitality industry continues to be vulnerable to data breaches and other cyberattacks. A report by Willis Group Holdings, a British insurance firm, states that the largest share of cyberattacks (38 percent) were aimed at hotels, resorts and tour companies. According to the report, insurance claims for data theft worldwide jumped 56 percent last year, with a bigger number of those attacks targeting the hospitality industry. Because businesses in the hospitality industry obtain and maintain confidential data from consumers–countless credit card records in particular–they will continue to be attractive targets for hackers and data thieves.

Cybersecurity risks can cause a company to incur significant loss or liability. A data breach could result in the loss of important and sensitive customer information and, in some cyberevents, stolen company funds. Companies also may face liabilities to third parties under statutory and regulatory schemes, incurring costs to mitigate, remediate and comply with the liability under these statutes. Worse still, class action lawsuits have been filed around the country after data breaches, with plaintiffs alleging, among others, the loss of the value of their personal information, identity theft, invasion of privacy, negligence or contractual liability. Even when companies have had success in defeating class actions, they nonetheless incurred significant legal expenses when defending those lawsuits.

Many businesses in the hospitality industry have undertaken important steps to reduce the likelihood of cyberattacks and to protect data and confidential information. Such measures are important, but equally important is understanding what insurance policies those companies have, or could purchase, to cover loss or liability associated with a data breach or other cyberattack.

Involving Technology and Privacy Managers in Insurance-related Matters Because of the variation in cyberinsurance coverages and the underwriting inquiries that often go along with the purchase of such insurance policies, companies may find the process to be a great opportunity for a company's risk managers, technology managers and privacy managers to work together to help understand potential risks to the company and what risk transfers are being purchased through the insurance policies offered. Working together aligns the risk managers' understanding of specific insurance-related issues, the technology managers' technical expertise regarding the companies' systems and protections that will be helpful to understand any technical requirements in an application or insurance policy, and the privacy managers' knowledge of the potential privacy risks that the company faces in light of the information held and how and where it is used. Indeed, given their understanding of the technical and practical considerations involved in protecting a company's data from a cyberattack, technology and information managers may be in a unique position to assist the company's risk managers in understanding the technical implications of specific policy language.

> Insurance claims for data theft worldwide jumped 56 percent last year, with a bigger number of those attacks targeting the hospitality industry.

Insurance Coverage Considerations When considering what coverages may apply or purchasing cyberinsurance coverage, it is essential to consider many types of coverage, as coverages often are written and offered in different modules and on varying insurance policy forms. On a regular basis, insurers are writing and introducing new policies marketed as being tailored specifically to cover data breaches and cyberattacks. In addition, coverage may be available under traditional forms of insurance. Indeed, policyholders may have overlapping coverage for data breaches and certain cyberrisks, with the potential for coverage under cybersecurity policies as well as traditional insurance policies. When analyzing the coverage afforded by such policies, it is critical to understand the impact of exclusions on coverages and any sublimits on the amount of coverage afforded by the policy. Because of the variety of coverages being offered, as discussed below, technology managers can assist the company by providing a careful review of the technical language used in the policy to help determine the scope and limitations of the coverage being purchased with respect to a specific company's operations.

Cybersecurity and Data Breach Policies The market for cybersecurity policies has been called the Wild West of insurance marketplaces. Such policies are relatively new to the marketplace and are constantly changing. Specific policies for cybersecurity and data breach have been known as Network Risk, Cyberliability, Privacy and Security or Media Liability insurance. The Insurance Services Office, Inc., which designs and seeks regulatory approval for many insurance policy forms and language, has a standard insurance form called the Internet Liability and Network Protection Policy, and insurance companies may base their coverages on this basic insuring agreement or they may provide their own company-worded policy form. Because these policies are frequently updated and changed, it is important to compare the coverages offered across companies and within a company's offerings.

Traditional Forms of Insurance Although it is ideal to purchase a policy designed specifically for cybersecurity risks, more traditional forms of insurance may also provide overlapping coverage for data breaches and cyberrisks, depending on the particular coverage terms and exclusions in the individual policy. Coverage may be provided by the following types of policies: commercial general liability; first-party property and business interruption; directors and officers or errors and omissions; crime; kidnap, ransom and extortion. Insurance companies, however, have been fighting their obligations to pay claims for cyber-related loss under such traditional insurance policies. A major insurer recently sued a corporate policyholder in New York, asking the court to rule that traditional insurance policies do not cover a series of high-profile data breaches, cyberattacks and cyberrisks.

Making a Claim for Coverage If a cyberevent occurs, such as a data breach, then it is vital that risk managers, technology managers and privacy managers work together to seek recovery under all potentially available insurance policies. It is recomended that policyholders 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. For example, under certain insurance policies, there is coverage for property damage and insurers have asserted that there has been no property damage as a result of a cyberattack. Technology managers, however, may be able to assist the company in marshalling 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). Technology managers should stay involved throughout the insurance recovery process to help assure that any representations and statements about the company's technology and the cyberevent are accurate and properly characterized.

A major insurer recently sued a policyholder asking the court to rule that traditional insurance policies do not cover a series of high-profile data breaches, cyberattacks and cyberrisks.

Beyond in-house technology personnel, companies that have sustained losses due to a data breach or cyberattack should consider speaking with an attorney who represents policyholders and has familiarity with this area. Because of the assistance of such lawyers, some policyholders have been able to obtain substantial recovery even after the insurer initially denied the policyholder's claim.

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 insurance companies. They may be reached at godess@dicksteinshapiro.com or trotterk@dicksteinshapiro.com. This information is general and educational and is not legal advice. For more information, please visit www.hospitalitylawyer.com.