Cybersecurity Insurance: Facing Hidden Risks and Uncertainty

By Clifford G. Tsan, Michael D. Billok and Franz M. Wright

Reprinted with permission from the May 2, 2016 edition of the New York Law Journal

Businesses and organizations are under increasing pressure to proactively and effectively manage cybersecurity risk. The costs of a data breach can be staggering. For instance, Home Depot recently agreed to settle putative class actions stemming from the company's extensive 2014 data breach by establishing a "cash plus" deal: Not only would Home Depot have to boost its data security practices and increase funding for identity protection services for consumers affected by the breach, the company also agreed to create a $13 million settlement fund to compensate consumers for out-of-pocket losses or unreimbursed expenses related to the data breach.

As another example, the data breach Anthem suffered in December 2014, which exposed nearly 80 million patient and employee records, has been estimated as likely to cost the company $31 billion. Faced with this stark new reality, companies and other entities are more frequently being encouraged to obtain cyber insurance coverage to help mitigate these risks, and it is critical that the consumer of such products understands their potential pitfalls.

Cyber insurance coverage is conceivably triggered by an entity's loss of confidential information or personally identifiable information, both electronic and non-electronic. Due to the rapid evolution of cyber-attacks, however, cyber insurance underwriters, brokers, and consumers have struggled with configuring the optimal insurance product to manage an entity's unique risks. This has led to fluctuating policy coverages and configurations. For example, some insurers offer policies that are written on a "stand-alone" basis, while others offer coverage through cyber-related provisions attached to other insurance policies, like an entity's general liability insurance plan.

A cyber insurance policy can include different types of coverages, such as third-party/liability coverage, first-party/theft of property coverage, or first-party/post-breach response coverage. These varied coverage types can insure against information security and privacy liability, regulatory defense and penalties, and crisis management expenses. Insurance policies may also contain a separate per-loss limit, a separate per-loss deductible, and an aggregate amount representing the maximum amount an insurer will pay for all covered claims.

For example, a policy may provide an aggregate limit of $20 million, but have distinct coverage limits for information security and privacy liability, and crisis management expenses. This complex structure requires that insureds understand their cyber risk before allocating their limited resources to various coverages. Insureds must also properly analyze their potential exposure in determining how much coverage they need; for instance, Anthem's $100 million cyber insurance policy was reportedly exhausted just by the mandatory notifications and free credit report monitoring it offered to victims of its data breach.

Moreover, companies often do not discover a data breach until an extended period of time after they have been hacked. For example, Excellus BlueCross BlueShield's data breach went undetected for nearly two years before being discovered in 2015. Insureds should therefore negotiate favorable retroactive dates in their cyber insurance policies to protect against any undetected data breaches that occurred before obtaining the policy.

Article I.Portal Healthcare Case

Case law addressing cyber insurance policies is still developing, and several recent cases have illuminated the complexities involved in navigating cyber insurance coverage issues. Most recently, on April 11, 2016, the U.S. Court of Appeals for the Fourth Circuit ruled in *Travelers Indem. Co. of Am. v. Portal Healthcare Solutions*, 2016 U.S. App. LEXIS 6554 (4th Cir. 2016) that Travelers is obligated to defend its insured, Portal Healthcare, in an underlying class action in New York stemming from Portal Healthcare's alleged failure to secure a computer server which contained confidential patient information.

The class plaintiffs had previously been patients at Glens Falls Hospital in New York, and alleged that their private medical records appeared in Google search results. Portal Healthcare held two commercial general liability (CGL) policies with Travelers that provided coverage for advertising or website injury resulting from electronic publication of information relating to "a person's private life."

Travelers commenced suit against Portal Healthcare in the Eastern District of Virginia and sought a declaration that the class action did not allege a covered publication because Portal Healthcare had not intended to publish the medical information and there was no evidence that any third parties viewed the information. Affirming the District Court's ruling in favor of Portal Healthcare, the Fourth Circuit squarely rejected Travelers' argument, holding that Travelers' duty to defend—which is broader than its duty to indemnify—was triggered by the class action's allegations that patients' private lives were exposed to "unreasonable publicity," as "any member of the public with an internet connection could have viewed the plaintiff's private medical records during the time the records were available online."

Article II. Other Cases

The Fourth Circuit's ruling in Travelers v. Portal Healthcare may provide insureds with new leverage in coverage disputes over data breach and other cybersecurity incidents, as it stands at odds with several other recent decisions supporting insurers' denials of coverage for data breach incidents. For instance, the scope of an insurer's duty to defend under a cyber insurance policy was a thorny issue in *Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs*, 103 F.Supp.3d 1297 (D. Utah 2015).

In Travelers, the insured had been sued in a prior action for wrongfully failing to return a client's customer account information, including credit card and bank information. The insured tried to invoke its "CyberFirst" policy's duty-to-defend provision and brought suit when Travelers disclaimed coverage. The policy provided that Travelers was obligated to pay for any damages or loss that was caused by the insured's errors, omissions, wrongful or negligent acts.

The U.S. District Court for the District of Utah held that Travelers was not obligated to defend because the related action against the insured alleged that it had "knowingly withheld" and "refused" to turn over the customer information, as opposed to a failure caused by errors, omissions, or negligence.

In another duty-to-defend case, *Zurich Am. Ins. v. Sony Corp. of Am.*, 2014 N.Y. Misc. LEXIS 5141 (N.Y. Sup. Ct. Feb. 21, 2014), a New York state court ruled that Zurich had no duty to defend Sony in litigation resulting from a 2011 cyberattack. Sony's commercial general liability policy included personal and advertising injury coverage for the policyholder's "oral or written publication in any manner of the material that violates a person's right of privacy." But the court reasoned that since the breached information was published by the hackers, not Sony itself, the insurer had no duty to defend as the policy required that the "publication" result from the policyholder's own actions.

Another coverage dispute is being litigated in *Ameriforge Group Inc., d/b/a AF Global Corporation v. Federal Insurance Co. and Chubb & Son*, No. 4:16-cv-00377 (S.D. Tex. Feb. 12, 2016), There, Ameriforge Group had suffered a $480,000 loss when criminals impersonating its CEO via email persuaded the company's accountant to transfer funds to a bank in China. In denying coverage, the insurer claimed that the original email, when sent, did not directly cause the company's loss; rather, it was the accountant's independent actions that resulted in the loss.

The insurer also claimed that the email was not an intrusive attack because it did not cause any loss or changes to the company's computer system and, although fraudulent, the email could have been received by anyone within the company. Although the U.S. District Court for the Southern District of Texas has not yet ruled on the legal merits of the insurer's position, its arguments for denial of coverage highlight some of the potential pitfalls in cyber insurance policies. Companies are targeted every day by phishing and social engineering attacks.

The federal government has also begun to recognize the significance of the cyber insurance marketplace. In a recent hearing before the House's Homeland Security Committee, representatives from the insurance and data security industries advocated for the creation of a central repository where companies could anonymously share information about cyberattacks. This data collection would benefit the cyber insurance marketplace by creating more definitive actuarial data from cyber incidents, and therefore lead to more robust cyber insurance guidelines and coverages.

The committee also heard testimony regarding the National Association of Insurance Commissioners' proposal to create a Draft Insurance Data Security Model Law, which proposes to harmonize state laws regarding data breach notifications for insurance companies and implement stricter rules in the event an insurer is hacked and confidential information is released. Uniformity in the data breach notification process could benefit both insurers and businesses operating in multiple jurisdictions because similar protocols would apply in the event of a data breach. This would enable businesses to more quickly respond to a data breach and mitigate their potential losses.

Efforts to create the repository and the Insurance Data Security Model Law are preliminary, but they foreshadow possible resources that may aid business entities in obtaining better insurance coverage in the cyber insurance marketplace.

In conclusion, insureds should obtain cyber insurance coverage to mitigate these risks, but also need to fully understand their policies and review potential gaps in coverage. Seeking competent advice in navigating this shifting landscape is crucial in properly managing an organization's cyber risk.

By Clifford G. Tsan, Michael D. Billok and Franz M. Wright

Reprinted with permission from the May 2, 2016 edition of the New York Law Journal

BOND SCHOENECK & KING ATTORNEYS

Commitment · Service · Value · Our Bond