TAG CYBER
LAW JOURNAL
JANUARY 2020

FOUR WAYS COMPANIES CAN GET SERIOUS ABOUT MANAGING CYBER RISK

With uncertainty roiling insurance coverage in this area, it's time for action.

BY DIANE D. REYNOLDS AND JOYCE E. BOYLE

Although cyber insurance has been available for nearly 20 years, it's still a relatively new and untested product compared to most other forms of property/casualty coverage. Decades of claims data on most types of natural and man-made hazards—ranging from hurricanes to careless driving—have enabled actuarial science to precisely measure risk and to assign well-reasoned pricing that protects the insured from financial ruin, while allowing the carrier to earn a return for assuming risk. But compared to fire, floods and robbery, cyber-related crime represents uncharted territory.

The knowledge gap involving cyber coverage is driven not only by limited claims experience. More significantly, actuaries have had no reliable means to calculate how quickly the penetration, complexity and sophistication of cyber crime will grow. Nor can they be expected to anticipate the depth and range of financial damage that cyber crime can cause.

Reflecting this experience—or lack of experience—a significant number of cyber-related claims have resulted in lawsuits that are now working their way through the courts.

Two Landmark Claims

The first two shots (bit.ly/37MM4Bk) across the bow of corporate America, and its reliance on insurance to hedge its exposure to cyber crime, involved large companies and significant damages. Zurich America challenged a $100 million claim by international food conglomerate Mondelez, and American International Group (AIG) denied a $1.3 billion claim filed by pharmaceutical giant Merck. Both claims resulted from the devastating NotPetya ransomware attack in 2017, which caused an estimated $10 billion in damages across the globe. At the time, the American and U.K. governments publicly blamed the Russian government for the attack.

The denials of the claims were notable in one respect. Both insurers rejected them on the basis that the NotPetya attack constituted an "act of war" by a hostile government—in this case, Russia—and were excluded as a result of the insurance policies' exceptions for acts of war. These were the first tests to determine the applicability of the act of war exclusion to cyber-related claims.

Both companies filed lawsuits challenging their respective insurance carriers' denial of coverage. The cases are currently pending in New Jersey and Illinois state trial courts. Although the act of war exclusion is contained in many insurance policies, courts have never addressed how it applies to coverage for cybersecurity incidents. Case law suggests that these landmark lawsuits may hinge on whether their insurance carriers can demonstrate that the attacks were perpetrated by a foreign government or a de facto governmental entity.

Courts have interpreted the exclusion in other contexts. The Ninth Circuit did so this year in *Universal Cable Productions v. Atlantic Specialty Insurance Co.*, and the Second Circuit took on the issue back in 1974 in *Pan Am World Airways v. Aetna Cas. & Sur. Co.* Both courts held that the act of war

exclusion only applies to the actions of foreign governments and nongovernmental actors, such as terrorist organizations and political activist groups, that have usurped power over land as de facto governments. However, given that numerous cyberattacks have been perpetrated by state actors such as Russia, North Korea and Iran, the lines between organized cyber crime syndicates and government entities have become blurred. This would seem to increase the chance that the exclusion will bar coverage for cyber claims, leaving businesses without cyber insurance coverage and significantly exposed.

Four Ways to Reduce Risk

So what can companies do? The single most effective way for companies to avoid the risk of cyber claims is to reduce the likelihood of a breach. Despite the growing threat of cyber crime, many companies have failed to safeguard against loss. While cyber insurance is certainly one way to protect a business, there needs to be a multilayered approach in creating a proactive cyber risk management program. Here are four ways that companies can reduce the risk associated with cyber claims.

Properly assess all cyber risks. Establish an interdisciplinary team of experts to conduct comprehensive cybersecurity risk assessment and determine what, if any, measures need to be taken to prevent or mitigate cyberattacks. This team should include various technical subject matter experts, including outside legal counsel. This will not only establish rigorous cybersecurity safeguards, it will also shield the process from discovery with attorney-client or attorney work-product privilege, in the event of litigation or administrative proceedings.

Implement serious cyber policies and procedures. Following its risk assessment, the interdisciplinary team of experts, including in-house lawyers, should create and oversee the implementation of new cyber risk management policies and procedures. It should also augment and improve existing cyber risk management practices, provide counsel with the most efficient means of allocating financial resources to support the cybersecurity initiative, and evaluate and weigh the benefits of technologies such as internet of things (IoT) devices and cloud computing against the cybersecurity risks they can potentially create.

Establish clear ownership of cyber risk management. Establish and staff a full-time role of chief privacy officer or chief information security officer (or both), and have them report to the CEO and the board of directors to oversee implementing and updating the company's cyber policies and procedures. These individuals should also oversee employee training, monitor internal cyber threats, and advise senior management on employment and labor laws related to employee monitoring and discipline related to cybersecurity. If there are budgetary constraints, these responsibilities must be clearly defined and can be assigned to established roles, such as the chief technology officer, chief information officer and chief legal officer, who must be held accountable for those tasks.

Work closely with your insurance broker and carrier. The interdisciplinary team should also assess the nature of the business, determine how it receives and stores information within its own system, and analyze what types of risks and financial exposure the company may face based on that data. The company should then coordinate appropriate insurance coverage with its insurance broker and/or carrier. Although large multinational corporations may appear to be the most inviting targets, corporations and institutions of all sizes have been victimized by cyberattacks.

The Bottom Line

The phrase that's kicked around most often regarding the growth of cyber crime is: "It's not a question of *if* your company will be attacked, it's a matter of *when* you'll be attacked." Acceptance of that defeatest premise, however, has resulted in too many companies failing to take cyber risk management seriously, resulting in significant financial exposure should an attack occur.

Regardless of how the Mondelez and Merck cases are decided, it's high time for companies to stop viewing themselves as inevitable victims of cyber criminals, and to address cyber risk management with the same level of attention and resources devoted to other critical corporate functions.

Diane D. Reynolds *is a partner at McElroy, Deutsch, Mulvaney & Carpenter and head of the firm's Cybersecurity, Data Protection, and Privacy practice. She has an extensive background in the representation of private and publicly held entities in corporate transactions.*

Joyce E. Boyle *is a partner at the firm with wide-ranging experience representing insurance carriers, including London market companies, in complex coverage and defense matters.*