A Moment of Truth for Cyber Insurance

By Ariel E. Levite, Wyatt Hoffman
Thursday, February 7, 2019, 9:21 AM

For many businesses, cyber risk was once either an amorphous threat or an occasional nuisance. But with reliance on all things digital skyrocketing, cyber threats now pose grave, even existential, dangers to corporations as well as the entire digital economy. In response, companies have begun to develop a cyber insurance market, offering corporations a mechanism to manage their exposure to these risks. Yet the prospects for this market now seem uncertain in light of a major court battle. Mondelez International is reportedly suing Zurich Insurance in Illinois state court for refusing to pay its $100 million claim for damages caused by the 2017 NotPetya attack.

Mondelez’s claim represents just a fraction of the billions of dollars in collateral damage caused by NotPetya, a destructive, indiscriminate cyberattack of unprecedented scale, widely suspected to have been launched by Russia with the aim of hurting Ukraine and its business partners. A compromised piece of Ukrainian accounting software allowed NotPetya to spread rapidly around the world, disrupting business operations and causing permanent damage to property of Mondelez and many others. According to reports, Zurich apparently rejected Mondelez’s claim on the grounds that NotPetya was an act of war and, therefore, excluded from coverage under its policy agreement. If the question of whether and how war risk exemptions apply is left to the courts to decide on a case-by-case basis, this creates a profound source of uncertainty for policyholders about the coverage they obtain.

Unlike physical attacks, the dividing lines between state-sponsored or state-abetted cyber aggression and organized cybercrime are far more (and often deliberately) blurred. Even when it is possible to attribute a cyberattack to a malicious perpetrator, it is much harder to confidently establish that a nation-state is complicit—as is often perceived to be the case with cyber aggression traced to perpetrators in the Russian Federation in particular.

This makes it more difficult for governments to determine when and how to step in to deter, respond to, retaliate against, or prosecute offenders even when they wish to. Governments already struggle to cope with cyber threats to their own assets and critical infrastructure, using limited resources. Governments are not inclined to assume more responsibility for addressing private-sector cyber risk, as it might encourage complacency, creating moral hazard. Consequently, companies must manage increasing exposure to cybercriminals and state-sponsored attacks on their own. At the same time, cyber risks increasingly cut across virtually all aspects of business operations, extending through relationships with suppliers, customers and business partners.

Many hurdles stand in the way of insurance providing a more robust solution. Data on cyber risks are scarce, and the threat is evolving constantly, often rendering data obsolete before they can be used. That means actuaries lack a credible repository of information to accurately price cyber risk. Moreover, NotPetya and other attacks with cascading effects have reinforced fears of aggregation risk, meaning the potential for a single incident to cause simultaneous losses across multiple policyholders. If Zurich had underwritten even a handful of the major corporations disrupted by the attack, it could have faced catastrophic losses from just one incident. This is a particularly acute concern for reinsurers—companies that provide stop-loss coverage, or protection against unsustainably costly claims, to other insurers—making both reinsurers and primary cyber insurance providers naturally hesitant to support more extensive cyber underwriting. The lack of adequate reinsurance backing means that carriers may become
overwhelmed with claims if a systemic cyber incident causes simultaneous losses across many policyholders.

Those turning to cyber insurance to manage their exposure presently face significant uncertainties about its promise. First, the scope of cyber risks vastly exceeds available coverage, as cyber perils cut across most areas of commercial insurance in an unprecedented manner: direct losses to policyholders and third-party claims (clients, customers, etc.); financial, physical and IP damages; business interruption, and so on. Yet no cyber insurance policies cover this entire spectrum. Second, the scope of cyber-risk coverage under existing policies, whether traditional general liability or property policies or cyber-specific policies, is rarely comprehensive (to cover all possible cyber perils) and often unclear (i.e., it does not explicitly pertain to all manifestations of cyber perils, or it explicitly excludes some).

But it is in the public interest for Zurich and its peers to expand their role in managing cyber risk. In its ideal state, a mature cyber insurance market could go beyond simply absorbing some of the damage of cyberattacks and play a more fundamental role in engineering and managing cyber risk. It would allow analysis of data across industries to understand risk factors and develop common metrics and scalable solutions. It would allow researchers to pinpoint sources of aggregation risk, such as weak spots in widely relied-upon software and hardware platforms and services. Through its financial levers, the insurance industry can turn these insights into action, shaping private-sector behavior and promoting best practices internationally. Such systematic efforts to improve and incentivize cyber-risk management would redress the conditions that made NotPetya possible in the first place. This, in turn, would diminish the onus on governments to retaliate against attacks.

In a recent Carnegie Endowment paper, we proposed a series of practical measures for insurers, corporations and governments to take—some separately, others together—to unlock the potential benefits of cyber insurance. These steps include upgrading the underwriting process, collaborating with cybersecurity services, and introducing specialized underwriting methodologies to better assess and price cyber risk. Governments, for their part, could help by developing common metrics for cyber-risk management, by encouraging companies to share information on cyber risks and security practices, and by standardizing corporate reporting requirements for cyber risk and data breaches. Sovereign wealth funds, holding companies and other major investors can also encourage responsible conduct by making regular, thorough cyber-risk assessments part of their due diligence.

Ultimately, the sheer magnitude of the challenge posed by cyber risk means that governments and insurers must work together closely. It should not be left up to individual companies or even to courts to determine state sponsorship for cyberattacks or to force Zurich and other insurance carriers to bear the full brunt of state-backed cyber aggression. Insurers need insulation from the most severe cyberattacks, regardless of their origins, in the form of a government backstop for catastrophic cyber risk, similar to the Treasury Department’s Terrorism Risk Insurance Program, which provides reinsurance for massive terrorist attacks. Such a backstop cannot come without requirements and preconditions, so governments and insurers must collaborate to find a realistic balance between their responsibilities.

The Mondelez-Zurich case underscores the urgency of government action to remove these barriers and address the risks that impede a more robust cyber insurance market. Doing so will be critical to unlocking the potential of insurance to diminish and channel risk, a role that has proved vital for managing traditional threats.

https://www.lawfareblog.com/moment-truth-cyber-insurance