Public Policy and the Insurability of Cyber Risk

Asaf Lubin

In June 2017, the food and beverage conglomerate Mondelez International became a victim of the NotPetya ransomware attack. Around 1,700 of its servers and 24,000 of the company's laptops were suddenly and permanently unusable. Commercial supply and distribution disruptions, theft of credentials from many users, and unfulfilled customer orders soon followed, leading to losses that totaled more than $100 million. Unfortunately, Zurich, which had sold the company a property insurance policy that included a variety of coverages, informed Mondelez in 2018 that cyber coverage would be denied under the policy based on the "war exclusion clause." This case, now pending, will be a watershed moment for the cyber insurance industry, highlighting the great ambiguity around the insurability of certain types of cyber risk and the scope of coverage that insurers will provide in the case of a cyber incident. The literature on the insurability of cyber risk has focused all of its attention on questions of economic efficiency and viability. Scholarship has, for example, examined the actuarial challenges in cyber risk modeling and the likelihood for adverse selection resulting from information asymmetries and lack of historical claims data. Scholars have so far avoided a different set of considerations rooted not in economics but rather in public policy analysis of societal values. This paper lays the framework for such an analysis. Relying on traditional insurance and torts jurisprudence the paper makes the public policy case for limited governmental intervention in the indemnification of four controversial categories of cyber harm: (1) acts of cyber terrorism or state-sponsored cyber operations; (2) extortion payments for ransomware attacks; (3) administrative fines for violations of statutory data protection regulations; and (4) disruption to supply, service, or distribution chains. In so doing, the paper highlights systemic challenges to cyber insurance underwriting while explaining insurers role in increasing societal cyber posture by reducing the likelihood of moral hazard and suboptimal cyber-norms enforcement.