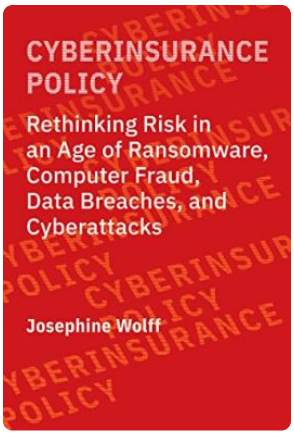
getabstract
compressed knowledge

Rating 8
Qualities
Eye Opening
Comprehensive
Hot Topic



Buy book or audiobook

Cyberinsurance Policy

Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks (Information Policy)

Josephine Wolff • MIT Press © 2022 • 296 pages

Management / Risk Management / IT Security
Industries / Insurance Industry

Take-Aways

- Cyber risks pose new, complex challenges to insurers, leaving companies vulnerable.
- The cyber insurance industry is unregulated and insures high-risk clients.
- Assigning blame for cyberattacks is challenging, as was evident after the 2011 Sony hack.
- A clearer definition of "computer crime" would benefit insurers and policyholders.
- It's difficult to dismiss cyberattacks as "acts of war," given their complexity.
- Insurers providing stand-alone cyber insurance policies struggle to name risks in dynamic contexts.
- Policymakers have a crucial role to play in strengthening cybersecurity efforts worldwide.
- Emerging technologies create emergent forms of cyber risk – insurers must reinvent policies.

Recommendation

The cyber insurance market faces growing pains, as computer systems are becoming increasingly embedded in all aspects of business and crime, says cybersecurity expert Josephine Wolff. Insurers lack a clear definition of cybercrime and are working in an unregulated industry without adequate support from policymakers, she explains. Wolff guides readers through the complex challenges emerging cyber threats present while making suggestions to policymakers and insurers regarding how to mitigate the impacts of mass-scale cyberattacks better.

Summary

Cyber risks pose new, complex challenges to insurers, leaving companies vulnerable.

NotPetya, one of the world's most destructive pieces of malware, took down computer systems at major US corporations in 2017, including consumer goods manufacturer Reckitt Benckiser and Deerfield, Illinois-based snack company Mondelez International. NotPetya took control of 10% of computers in Ukraine, leading to suspicions of Russian military involvement. The insurer Zurich refused to pay out Mondelez's claim, arguing that it wasn't responsible for damage or losses caused by "hostile or warlike action in time of peace or war." The logic behind Zurich's exclusion wasn't clear-cut: Was a cyberattack on the US manufacturer of Oreo cookies and Ritz Crackers an act of war? The case remains undecided today, as Zurich pursued settlement negotiations outside of court, drawing attention to the complexities and ambiguity in the cyber insurance industry.

> *"Insuring cyber risks is a fundamentally risky proposition at a time when there is still so much we do not know about the threat landscape."*

Cybersecurity risks differ from other forms of risk in a critical way: Insurers rarely find themselves having to pay out multiple claims simultaneously, yet cybersecurity attacks can occur across industries, hitting multiple players at once. Since the cyber insurance industry emerged in the 1990s, insurers have dealt with the unusual nature of cyber risks by isolating risks using stand-alone policies. But doing so is a questionable tactic, given that data and computer networks are embedded into other systems, impacting other coverage areas in complex ways.

The cyber insurance industry is unregulated and insures high-risk clients.

In 1997, Steve Haase steered the creation of the Internet Security Liability (ISL) policy, a policy designed to cover emerging e-commerce risks, underwritten by the American International Group (AIG). Haase was working with a lack of actuarial data, and ISL's premiums started at only $2,500 per year – with a 25% discount for companies with a National Computer Security Association certification. Today, such low prices would be unthinkable: By 2017, just 471 firms with cyber insurance policies reported more than $3 billion in insurance premiums in the swiftly growing industry. The price of annual premiums has varied wildly in the 2000s, with some paying over $100,000 (Gartner, for example, charged $125,000 for its $25 million coverage policies in 2000). The rapidly expanding industry is mostly unregulated today, with

no governing body defining baseline requirements of what cyber insurance policies need to cover and for whom.

> *"Unlike other forms of insurance, there are no requirements governing what cyberinsurance policies must cover, who must obtain them, or to whom they must be made available."*

In 1869, the US Supreme Court ruled that the same laws of commerce didn't govern insurance, as it was "not a transaction of commerce" (*Paul v. Virginia*). This logic made insurance a difficult industry to regulate, which US Representative John Dingell attempted to change in 1990, arguing (in the House subcommittee report "Failed Promises: Insurance Company Insolvencies") that American insurance companies could cheat their customers and fail to meet promises. Dingell called for more regulation, critiquing the industry's low barriers to entry, as capital wasn't needed to make promises. In 2003, California began legally requiring companies to disclose when data breaches had occurred, creating mandated reports that helped the public better understand the reality of cybersecurity risks. Yet despite subsequent regulations from the Securities and Exchange Commission (SEC) expanding the scope of the disclosure, insurance carriers today appear less invested in assessing clients' risk levels, gambling that high volumes of premiums will enable them to pay out claims.

Assigning blame for cyberattacks is challenging, as was evident after the 2011 Sony hack.

After Sony successfully sued 19-year-old George Hotz – a user who'd discovered a way to modify its PlayStation consoles to play games from other companies – they received an ominous warning from the hacker group Anonymous. "You have abused the judicial system in an attempt to censor information on how your products work," asserted the hackers, adding: "Now you will experience the wrath of Anonymous." Sony failed to safeguard its network adequately, and in 2011, a hack to the Sony PlayStation Network compromised 77 million user accounts, exposing details including credit card numbers and passwords. This massive data breach triggered two separate legal battles: Sony's customers filed a class action lawsuit in California, accusing the company of negligence, and one of Sony's commercial general liability (CGL) insurers, Zurich, sued Sony in a New York Court after Sony tried to use its liability coverage to pay its legal fees.

> *"Deciding who to blame was far from straightforward and depended a great deal on the particular details of any given incident."*

Sony made two contradictory arguments in both courts: To the customers suing it for negligence, Sony argued that it was not at fault and was itself a victim of the hackers, too, given that "there is no such thing as perfect security"; Sony simultaneously argued it was "at fault" when attempting to use its liability insurance. Sony's security was far from perfect: For example, while it encrypted users' credit card details, it didn't encrypt other data, such as passwords. Sony paid $15 million in 2014 to settle a class action lawsuit with its customers. New York judge Jeffrey Oing ruled that Sony wasn't covered by its CGL policy, as it wasn't intended to cover third-party liability or intrusions. Both court cases reveal the difficult challenge of properly establishing fault in complex cybersecurity cases. If baseline cybersecurity practices and measures

existed, it would be easier to establish a level of "no fault" insurance to properly compensate victims and reduce confusion.

A clearer definition of "computer crime" would benefit insurers and policyholders.

The 2008 arrest of Bernie Madoff, who defrauded investors of $65 billion, exposed one of history's biggest Ponzi schemes. The Louisiana-based Methodist Health System Foundation Inc. (MHSFI) attempted to recoup an estimated $439,467 in losses for their investments by filing a claim with its insurer Hartford, hoping the claim would fall under the "Computer and Funds Transfer Fraud" portion of its Crime Shield Policy. MHSFI argued that Madoff had used a computer to fraudulently create official-looking month-end statements and trading slips, thus making Madoff guilty of computer fraud. Hartford denied the claim, explaining that since MHSFI had invested in Madoff's scheme voluntarily, they knowingly took a risk and weren't computer fraud victims "within the meaning of the Hartford Policy." Although Madoff was sentenced to 150 years in prison and pleaded guilty to 11 counts of fraud, the US District Court didn't find him guilty of computer fraud.

> *"Computer fraud, and cybercrime more generally, has proven a challenging category of risks for insurers to define clearly, both because there is a wide variety of mechanisms for executing fraud through computers, and these mechanisms are constantly changing, and because cybercrimes often overlap with other types of theft."*

Madoff's case draws attention to the murky definition of computer fraud due to the increasing prevalence of computers in various criminal and business activities. Insurers have different interpretations of computer fraud, resulting in uncertainty for policyholders. There's a need to break computer fraud into specific categories, encompassing the diverse uses of computers while simultaneously limiting the potentially broad scope of computer fraud.

It's difficult to dismiss cyberattacks as "acts of war," given their complexity.

Both NotPetya and the North Korean government-backed breach of Sony Pictures raised concerns about whether one can consider a computer code a war act. After all, NotPetya's damage to companies, like US snack food manufacturer Mondelez, didn't endanger anyone's life. Likewise, US President Obama explicitly stated that he didn't think the Sony Pictures hack constituted an act of war but instead referred to it as "an act of cyber vandalism that was very costly, very expensive."

> *"Classifying cyberattacks according to the kind of damage they do to data or critical infrastructure has several advantages over trying to categorize them based on their perpetrators and broader political context."*

In a 2020 study of 56 cyber insurance policies, Daniel Woods and Jessica Weinkle noted a trend of introducing cyberterrorism coverage in policies. Yet insurers have done so in vague terms while weakening the impact of existing war exclusions. Generally, companies can only make war exclusions if they can identify the perpetrator and motive, which may not always be possible or realistic today. Unlike war exclusions, cyberterrorism exclusions focus more on verifiable factors, such as the attack's impact on

victims. However, there's a large degree of uncertainty and disagreement regarding what constitutes cyberterrorism, as opposed to less severe forms of cyberattack. Insurance companies would fare better if they more clearly defined cyberterrorism exclusions, excluding coverage for large-scale cyberattacks in language that specified the associated impacts, victims and scale.

Insurers providing stand-alone cyber insurance policies struggle to name risks in dynamic contexts.

In 2015, insurers began selling more stand-alone cyber insurance policies, covering costs associated with activities like data breaches, extortion and network outages. Premiums for stand-alone policies rose by 379% between 2015 and 2019, with sales climbing from just over $480 million to $2 billion. Insurance carriers faced three major challenges when developing these policies: A lack of consistency in data collection, an inability to effectively limit or assess customers' cyber risk exposure and the pervading possibility of cyber risk on a massive scale. Insurers took a "named peril" approach in that they specified numerous risks and third-party costs the insurer would cover. Insurers have also narrowed the scope of risks covered, increasing the number of explicit exclusions in stand-alone policies. Given the ever-evolving nature of cybercrime, policyholders still face uncertainty regarding whether they'll be covered for online threats in the future.

> *"In trying to treat cyber as a risk analogous to cars, floods, fires or property, by creating stand-alone coverage, insurers actually undercut their ability to use the wide range of different coverage formats and risk-modeling tactics at their disposal to address different facets of cyber-related risks."*

There's no clear indication whether a named-peril approach will be advantageous to insurers or policyholders in the future due to the dynamic, rapidly changing context cyberattacks exist in. Likewise, offering comprehensive cyber insurance plans seems unwise, as insurers could wind up liable to cover more accumulated risks than they have the means to. Insurers would benefit more from creating different categories of insurance to cover varying types of risk, much like insurance policies associated with electricity.

Policymakers have a crucial role to play in strengthening cybersecurity efforts worldwide.

Despite mounting pressure in both the United States and EU on policymakers to play more of a role in the cybersecurity landscape, there's still a lack of clarity surrounding the state's role in working with cybersecurity insurers. Daniel Woods and Andrew Simpson created a framework for policymakers (published in the *Journal of Cyber Policy*) proposing they enact cybersecurity policies in the following six areas:

- Initiating or standardizing data collection.
- Defining coverage areas better.
- Pushing for broader cyber insurance adoption.
- Promoting information sharing with the aim of improving insurers' risk models.
- Clarifying or imposing best practices.
- Responding to cyber damages that occur on a catastrophic scale.

> *"If policymakers are waiting for cyber insurance to become more widespread, standardized, stable and effective at strengthening private-sector cybersecurity before acting to regulate it, they must also face the possibility that insurers may not be able to achieve those goals without the assistance, support and restraints of government regulation."*

In 2020, the United States CyberSpace Solarium Commission recommended that the government fund a cybersecurity research and development center. The center would support state regulators in setting minimum cyber insurance policy standards, as policies vary by state. The Commission also suggested the US government "explore the need for a government reinsurance program to cover catastrophic cyber events" and released a draft bill to Congress with legislative proposals. Although Congress didn't act on this bill, the Commission created momentum in global discussions surrounding cybersecurity.

Emerging technologies create emergent forms of cyber risk – insurers must reinvent policies.

Moving forward, policymakers can support cyber insurance companies in the following ways:

- Covering the costs of massive-scale cyberattacks.
- Aggregating anonymized data related to cybersecurity claims from insurers to aid in creating risk models.
- Prohibiting insurers from paying extortion demands, such as ransoms, to avoid fueling organized crime.

> *"The idea that cybersecurity can be handled solely, or even primarily, through a market-driven approach led by insurers is fundamentally flawed – something that insurers themselves, to their credit, have been pointing out to policymakers for years."*

Cyber risks of the future will be more intertwined with other forms of risk, and stand-alone policies will no longer suffice in their current form. The potential for hackers to target users through smart home devices, health devices or autonomous vehicles is radically disrupting the insurance industry. New intermediaries and stakeholders are emerging, and those designing insurance for new products and devices won't be able to rely on existing policies. Not every risk is a cyber risk, but there is a cyber dimension of all types of risk – those who ignore this fact do so at their peril.

About the Author

Josephine Wolff is a Tufts University associate professor of cybersecurity policy and the author of *You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches*.