Private-Interest Cybersecurity Governance: The Case of Cyber Insurers

By Ido Sivan-Sevilla

Private-Interest Cybersecurity Governance: The Case of Cyber Insurers

By Ido Sivan-Sevilla – ***Postdoctoral Fellow at Cornell Tech's Digital Life Initiative***

Scholars of cybersecurity governance usually study government regulations or self-regulatory arrangements when assessing how ICTs are protected from unauthorized access. Less attention is devoted to the increasingly important role of private governance actors in this space (e.g. insurance companies, certification bodies). These actors are acting as 'rule-intermediaries' between governments/corporations [rule-makers] and those who collect, process, and use our data [rule-takers]. In the case of cyber insurers, their rule intermediation includes taking over 'rule-making capacities' over the assessment, prevention, and mitigation of data breaches. This is happening with no public oversight, and thus requires a close examination for tracing trends and biases in how insurers decide to protect our data.

As private actors, insurance companies are led by financial interests when deciding on the risk-taking strategy of their clients. Scholars, however, mostly praise the involvement of the insurance industry in the cybersecurity space, stating how insurers are fulfilling state regulatory vacuums (Talesh, 2018) and shifting corporate incentives to invest in privacy and security (Levite et al., 2018). I argue in contrast, that we should be critical about the way insurers choose to govern data breaches. In practice, we see how insurers fill gaps in data security and privacy guidelines by institutionalizing their own practices in ways that might jeopardize the public interest. They bound insureds to certain security providers, set unclear criteria for who is eligible for cyber insurance, institutionalize cybersecurity practices without clear scrutiny by others, and engage in risky behaviors that put clients and their (our) data at risk.

The threat of a data breach is one of the most alarming threats corporations are currently facing (e.g. Popomaronis, 2020). The financial stability and public reputation of companies can be rapidly affected by a successful breach. It is not surprising though, that companies choose to shift some of those risks to the vastly growing cyber insurance industry. Organizations seek data security practices to follow, experts to consult with, and financial compensation in case data breach risks turn into a reality. The risks to the privacy of their clients and the security of their IT infrastructures are translated into business opportunities by the insurance industry. Insurers take advantage of the fact that they work in an environment where mandatory data security regulations are largely absent and introduce their own set of data governance practices. The vulnerable nature and inherent insecurity of digital infrastructures (e.g. Timberg, 2015) make the need to comply with data breach notification laws a necessity across economic sectors (for a cross-sector analysis of data breaches see Huq, 2015). By buying insurance policies, companies seek some clarity in this uncertain environment. Gradually and consistently, cyber insurers are not only deciding on the meanings of privacy compliance post-breach, but also choose for their clients preventive

data security practices to follow, operating way beyond the scope of what insurers typically handle - pooling risks across policyholders (Marotta et al., 2017).

The institutionalization of cybersecurity practices by the insurance industry is happening with no public oversight. Insurance is supervised by state regulators, who traditionally inspect the financial solvency of insurers and the level of consumer protection they provide, to ensure the adequacy and fairness of policies. The ways insurers choose to manage risks for their clients can potentially create bias on how our data is protected and requires a much closer inspection.

Surprisingly, the cyber insurance literature is almost unanimously enthusiastic about this stretch in the role of insurers. The facilitation of risk prevention and mitigation practices by the industry are perceived as improving organizational practices and compliance capacities of insureds (Talesh, 2018). Insurance companies are understood as fulfilling a vacuum for organizations that perceive themselves as unprepared for a data breach (Herr, 2019). Cyber Insurance is perceived as a proper substitute for state governance and as an intervention that fundamentally reshapes 'the already-difficult cyber risk landscape' (Levite et al., 2018). Scholars also applaud the extent that the insurance industry can potentially motivate the behavior of its clients and help reverse trends of insufficient security investments by companies (Talesh, 2017). The thrive of the cyber insurance industry is framed as a solution to information-sharing difficulties in this landscape: 'Insurance companies can accumulate data about breaches and then develop and share insights about the factors that shape the risky environment, operating as a central repository for granular data relevant to data security and privacy challenges of actors across the economy' (Levite et al., 2018). Following this sympathetic trend in the literature, many works are devoted to finding the optimal conditions for a successful cyber insurance market. Suggested solutions for that include government backstops for 'cyber catastrophes,' facilitation of information-sharing between insurers, standardization of policies, and utilization of governments' procurement power (see for instance: Woods and Simpson, 2017). These works falsely assume that the wide spread of cyber insurance means better security for our data.

The literature mostly ignores the potential bias of managing data security and privacy risks by a private-interest industry. Preventive measures, compensation for losses, and possibilities to engage in risk-taking practices are all dictated by a for-profit industry that might push data practices of companies in ways that undermine social welfare. Should we give so much deference to insurance companies without evaluating and assessing winners and losers from their operations? Before I detail why the answer is 'absolutely not' and present what I am already recognizing as 'insurance-biased risk governance practices,' the following paragraphs trace the growth of insurers as cybersecurity governors and overview how they gather responsibilities for the security of our data.

Cyber Insurers as Governors ‘Beyond the State’

The fact that insurance experts ‘teach’ insureds the habits of risk prevention or ‘translate’ for them the meaning of regulatory compliance is nothing new (for a historical critical analysis on insurers as governors see Ericson et al., 2003). More often than not, ‘insurance takes an active role in the development and implementation of loss prevention infrastructures’ (Doyle and Ericson, 2004, p.289). In the property insurance market for instance, insurers set up the first fire departments following the Great Fire of London in 1666 (Read, 2016). The role of insurers as risk preventors was also evident in the early days of maritime trade, in which Lloyd’s of London created a market for insurance to address associated risks (Bogardus Jr., 2007). Today, product liability insurance drives monitoring of food safety standards and environmental insurers help clients avoid costly damages and comply with regulatory standards (Ben-Shahar and Logue, 2012). These are few examples of insurance companies governing clients ‘beyond the state,’ following a liberal theory of governance that de-emphasizes states’ responsibility (e.g. Rosenau and Czempiel, 1992).

The popularity and significance of the cyber insurance industry have been gradually evolving. In 1997, AIG wrote the first-ever cyber insurance policy. But the industry had significantly grown only after the introduction of states’ data breach notification laws in the beginning of the 2000s (Marotta et al., 2017). These transparency requirements created an incentive for companies to get insurance in order to compensate their clients (the ‘third-parties’ in this case) following privacy harms from data breaches. Third party coverage typically included costs associated with class-actions lawsuits or settlements (Wolff, 2018). Gradually, insurance companies moved to additionally cover first-party damages of the insured. This can include coverage for online extortion payments, renting temporary facilities during a cyber-attack, and lost business due to system failures (Solove, 2018). Recently, the insurance industry is also partnering with security vendors in trying to prevent data breaches all-together, to reduce the industry’s financial risks. Insurers require security standards in line with certain best practices and offer recommendations on useful security software.

This expansion in the roles of insurance companies came with a steadily increasing demand for cyber insurance by the market. In the year of 2018, direct premiums written for cyber insurance packages grew by 12 percent to $2 billion. This rate has doubled since 2015 (A.M Best, 2019). Today, more than 500 US carriers are offering cyber insurance (Grones, 2019). The total number of cyber insurance claims in 2018 was 12,532, a growth of 39 percent from the same number in 2017 (A.M Best, 2019). While the market is not growing according to initial predictions (e.g. Böhme and Schwartz, 2010), the industry is experiencing spikes that we do not often see in other insurance sectors (Wolff, 2018).

The growth in insurers' market share alongside their new assigned roles within covered organizations raise two fundamental questions: (1) How insurers practically intervene in the cybersecurity governance practices of their clients? (2) should we be worried? (Disclaimer: Yes). To detail more on the first question, insurance companies both orchestrate data breach mitigation practices (after a breach occurred) and dictate steps for assessing and preventing the risk. The first role of 'post-breach services' is considered by many as the 'success story' of this industry (e.g. Woods and Moore, 2019; Talesh, 2018). Cyber insurers practically shape the way their clients respond to a data breach. They cover the forensic, restoration, crisis management, and credit reporting expenses, driving the entire incident-response strategy of the company including public-relations aspects (Talesh, 2018). Issues that arise during a breach are guided by insurance industry professionals or third-party vendors that insurers match for their clients at a reduced fee (Talesh, 2018).

In their second and more recent role, cyber insurers engage in providing tools and guidelines to assess and prevent the risks in advance (Romanosky et al., 2019; Wolff, 2018). Insurance intervenes in two phases of the risk governance process: For risk-assessment, insurers conduct security questionnaires related to the security systems in place, assess the compliance levels of their clients with certain standards, and evaluate the assets and threats insureds are facing. The industry also looks at more 'hidden' risks by scanning publicly-facing infrastructures (Talesh, 2018). For risk-prevention, insurers are setting the bar for data security practices as required pre-conditions to qualify for insurance (Camillo, 2017). The expensive coverage the industry offers leads insurers to introduce their 'own' risk prevention services (Talesh, 2017), as the validity of the insurance policy often depends on implementing prescribed security control (Woods and Simpson, 2017). By influencing the ways their clients assess and prevent data breach risks, insurers absorb some of the traditional responsibilities of internal IT departments (Talesh, 2018).

To support the risk governance operations that insurers promote, the industry partners with third-party security service providers. These contractors are stepping into companies under the facilitation and regulation of insurers, creating an additional level of out-sourcing in the handling of data breach risks. The German insurer Allianz for instance, has a partnership with Aon, Apple and Cisco. Allianz customers can receive 'enhanced' cyber insurance policies, including lower deductibles, if they 'use assessment tools, security technologies, and breach response services provided by their partners' (Wolff, 2018). Another example is the partnership between the insurance company Chubb and the security service providers CrowdStrike and FireEye. Clients that work with these contractors get a preferred premium rate. Additional examples include the partnership between AIG, CrowdStrike and Darktrace to improve risk assessment (Herr, 2019) or the Zurich insurance company that provides customers with access to Deloitte's cybersecurity consulting services.

Captured Cybersecurity Governance?

The cyber insurance industry grows and ascribes itself an increasing number of governing roles, sometimes fully capturing organizational decision-making over cybersecurity governance, with no public oversight. As an increasingly dominant actor, it becomes especially important that insurers would not limit possibilities for data protection, set fair and transparent criteria for insurance eligibility, properly incentivize companies to invest in data security, and engage in non-risky behaviors in the unpredictable domain of online threats.

Preliminary findings, however, suggest otherwise. Buyers of cyber insurance often partner with certain vendors, according to the insurer's terms, and are bounded to specific information security practices that these vendors can offer (Talesh, 2018; Woods and Moore, 2019). Since there is no bullet-proof recipe for assessing, preventing, and mitigating data breach risks, it is still far from clear that insureds enjoy a variety of options to protect themselves. In contrast, it seems that certain powerful security contractors (e.g. CrowdStrike) are further increasing their influence thanks to the insurance industry, leaving blind spots in the ways IT infrastructures are protected.

Moreover, the criteria for who gets the possibility to become insured remain unclear. The insurance industry establishes the underwriting criteria and charges premiums based on various risk-profiles and risk assessments in ways that might prevent small/medium businesses from purchasing insurance. Without public oversight, it is the insurers who get to control who can and cannot obtain insurance (Talesh, 2018). In the risky environment of online threats, certain data companies that cannot afford insurance might not be able to compete with those who can. Should the industry set non-transparent criteria and deny insurance from companies? Is data insurance a privilege only the rich and powerful can enjoy? Or is there a public interest in making the protection of our data insured? The US regulatory system currently agrees with the former, but as data become pervasive and identity theft rise, this position should be revisited, to say the least. Ericson et al. (2003) argued that 'insurance is political' since it un-pools risks by segmenting the market according to its own interests. This political power should be addressed in the cyber insurance space as well.

The insurance industry might also push firms to under-invest in ex-ante security controls, paving the way for insurance-led security practices to dictate cybersecurity governance efforts. Empirical evidence shows that the moral hazard in transferring data breach risks from companies to insurers is rarely addressed. Price premium discounts are often unrelated to data security steps taken by the soon-to-be insured (Romanosky et al., 2019). Moreover, companies are beginning to demand from each other to carry insurance as a requirement of doing business (Herr, 2019), further institutionalizing insurers' risk treatment as the 'accepted' norm to protect data.

But maybe the most troubling aspect is the fact that market pressures push insurers toward a risky behavior. Insurers are driven by financial motives rather than by the purpose of protecting clients' data. There is a steady stream of new and risker coverage offered by the industry, as insurers provide higher policy limits for new issues (Herr, 2019; Solove, 2018). Increased competition within the insurance industry has resulted in an expansion of coverage, and it is unclear how this impacts the profitability of the industry or the security of our data. Competitive pressures, for instance, drive a race-to-the-bottom in risk assessment practices and prevent insurers from including security procedures in contracts (Woods and Moore, 2019). The increasingly expensive coverage creates space for insurers to offer their own risk management services to combat the various risks that they choose to insure and institutionalize their own bias on how the handle those risks. Insurers are racking up higher and higher premiums and 'crossing their fingers, trying all kinds of gimmicks to get the companies they are underwriting to clean up their acts' (Doctorow, 2018).

Conclusion

Cyber insurance is much more than a 'traditional' insurance mechanism. Instead of just pooling the risk across policy holders, cyber insurers assess, try to prevent, and manage those risks, often instead of their clients. This expansion in the role of insurance calls for careful attention. We already witness how cyber insurers pose their own risk assessment and prevention methods, tie clients to specific vendors, and accumulate power by solely deciding who is eligible for insurance. Financial motives are leading insurers to risky behaviors, and without public scrutiny, data subjects might pay the price.

Can we rest assure that insured entities are properly governed by a private insurance industry? Absolutely not. As the cyber insurance industry becomes more powerful, the interests of data subjects are second to economic motives at best. Some insurers promise more coverage and secure our data based on 'insurance-best practices' that are rarely visible to the public. The US neo-liberal paradigm of governance created big tech. The same paradigm is now fueling an 'insurance-tech' industry, in ways that are dangerous to our public interest.

Ido Sivan-Sevilla
Digital Life Initiative