A Turning Point for Cyber Insurance

A Turning Point for Cyber Insurance

Daniel W. Woods

April 13, 2023

Abstract

For the first two decades, the cyber insurance market rewarded entrepreneurial insurers who embraced uncertainty (or ignorance) while offering innovative insurance products. The supply increased as insurers expanded into the new product. Applicants and brokers began to seek out those underwriters who had the lowest underwriting standards and price, which preventing informed insurers from applying their expertise. Ransomware shattered this equilibrium, creating space for insurers—both traditional carriers and start-ups—who can accurately price risk and nudge policyholders towards better security. Looking forward, we should expect technologists who can understand and measure cyber risk to thrive.

Article

Insuring against the consequences of cybersecurity seems too good to be true given the underlying problem has perplexed researchers and practitioners for going on fifty years. Since the 2000s, firms could purchase a *cyber insurance* policy with coverage items including data breach litigation, crisis management services, data restoration and, controversially, ransom payments. The National Association of Insurance Commissioners (NAIC) estimate that the number of policies in the US grew from 2.1 million in 2016 to 4 million in 2020 with policyholders paying $2.75 billion in premium [1].

Recent years have seen cyber insurers struggle. The NAIC reports on a 400% increase in ransomware incidents and that three of the top four cyber insurers had unprofitable loss ratios—claims paid out as a percentage of premiums collected [1]. The industry is responding by reducing coverage limits and hiking premiums, anticipated to be a 15-50% rise in 2021 [1].

As a computer scientist, it is easy to interpret such reports as the death of an industry. Finance professionals waded into a technical problem that they did

Author copy. The reference details of the final published version are:
Daniel W. Woods. 2023. A Turning Point for Cyber Insurance. Communications of the ACM 66, 3 (March 2023), 41–44. https://doi.org/10.1145/3545795

not understand and got burnt by the reality of cybersecurity, therefore it was inevitable that insurers would either stop offering coverage or invoke exclusions to avoid paying out on any claims. This story has elements of truth, but also belies a folkish and naive understanding of insurance markets. I argue that the industry's pain is evidence of the fundamental value of insurance—it pays out when policyholders suffer harm—and that, over time, this dynamic will push the ignorant cyber insurers out of the market. This creates space for technology-focused professionals and solutions.

Beginnings To understand how so many insurers sold cyber coverage without understanding the underlying risk, it is important to go back to the beginnings. AIG, who would later be bailed out by the US Government during the 2008 financial crisis, released their first cyber insurance long before cyber-attacks dominated headlines [2]. Without any historical loss data to analyse, the underwriters made assumptions about how business interruptions caused by Distributed Denial of Service (DDoS) attacks compared to well understood disruptions caused by fire. AIG's Chief Operating Officer, Ty Sagalaw [2], later admitted that the risk model was "a complete guess." Here, we see the trope of greedy financiers wading into a technical problem they did not understand.

Nevertheless, Sagalaw claims the company sold $100 million worth of cyber insurance and paid out around 10% of that in claims [2], a wild success. It is an open question whether early profits resulted from a deeper understanding of cyber risk, a favourable threat landscape, or elevated prices to account for initial uncertainty. The product changed over time, shifting towards covering litigation and response costs resulting from data breaches [3], but generally cyber insurance remained a niche, profitable line of insurance. Underwriters assessed cyber risk using more art than science, many operating out of the Lloyd's market—the infamous market where David Beckham insured his foot.

Growth This success was ultimately the market's demise. Non-specialists took note and began offering cyber coverage. This resulted in cyber insurance prices falling in real terms from 2008 to 2018 [4]. Regulatory filings in the US reveal many insurers copied pricing plans from competitors [3]. The influx of pretenders reduced the cyber insurance industry's understanding of the underlying risk.

This led to a situation in which the main methods of risk assessment would have been familiar to insurers from before the IT revolution. Applicants were asked to fill out paper questionnaires about network security practices [5]. Critics held that questions such as "[d]o you have a firewall?" abstracted away from the daily grind of configuring and maintaining corporate networks. A practitioner I know described these application forms as an exercise in "how to lie the least."

Another option was to conduct underwriting calls [5] in which multiple insurers would ask questions like "where and how do you store customer personal data," to which the finance team would whisper to each other and say they will get back to the insurers on that one. Many questions went unanswered unless an employee with technical expertise was on the call. If an underwriter sensed a problem, brokers would simply find an insurer asking fewer or less technical

questions.

Some insurers became uncomfortable with the situation. As the growth line of insurance, cyber attracted the most ambitious professionals, many of whom studied part-time for masters degrees or InfoSec certifications. But insurers who developed a feel for effective security controls faced a problem [4]. They either offered coverage based on less-than-perfect risk information or saw that premium go to a competitor asking fewer questions. Market conditions meant that even informed insurers could neither collect the relevant underwriting information, nor require that policyholders put controls in place. This left cyber insurers exposed to the problems of adverse selection and moral hazard, which are known to drive sub-optimal security outcomes [6].

Ransomware The status-quo held while data breach litigation was the main cost driver, but then a ransomware epidemic began. Ransomware gangs brought businesses to their knees demanding payment. While critics of the industry contend that insurers were too willing to pay and this caused ransom inflation [7], insurers counter that paying ransoms saved businesses from going out of business. Either way, the ransomware gangs re-invested revenues, expanded capacity, and began demanding higher ransoms. One ransomware negotiator reports 1000% year-on-year growth in the mean ransom payment [8]. This led some cyber insurers to stop covering the cost of payments to ransomware gangs.

This brings us to the present, in which some insurers paid out more in claims than they collected in cyber insurance premiums, before operational costs are counted [1]. So far, the InfoSec narrative of greedy financiers seems to hold. However, the narratives fail to appreciate how insurance markets create evolutionary incentives. The ransomware epidemic is a force that disproportionately punishes insurers with relaxed underwriting standards. Many of the insurers with unprofitable loss ratios are restricting coverage and even leaving the market. This creates space for novel business models based on understanding cyber risk. In the following, I outline three such directions for innovation.

Rewarding Security Insurers can take advantage of the market conditions caused by the ransomware epidemic to improve social welfare by offering incentives for better security. A movement in this direction can be seen in emerging reports about policyholders facing deeper assessments and stricter requirements. Cyber insurance purchase and renewal is now conditioned on implementing "multi-factor authentication (MFA) as well as endpoint detection and response" [9]. However, insurers can only exert this influence before a contract is signed, which typically lasts a year, during which time the threat landscape could change. This is especially problematic when new vulnerabilities emerge during the policy term.

An innovative approach is to continually scan policyholders. One venture capital funded cyber insurance provider reports that "scans for vulnerabilities and ports exploited by ransomware groups resulted in a 65% drop in ransomware-related claims from April to September 2020" [7]. The underlying technology typically involves scanning public facing servers, which can be collected at near zero cost to the policyholder (unlike questionnaires or video calls). The next research and industry challenge is how to probe deeper into

networks without imposing a cost on policyholders.

It may be tempting to socially engineer employees to test security awareness, but this creates costs in terms of lost trust, emotional stress and wasted time. Similarly, clumsy probes could cause costly down-times for industrial control systems. I believe the answer lies in collaborating with technology providers like cloud providers, MSSPs, network monitoring vendors and so on. The precise business model is an open question, but these firms are clearly best placed to assess and help reduce cyber risk. It could look like insurers acquiring security vendors, cyber insurance as an add-on to a cloud computing subscription, or even InfoSec vendors offering to pay the costs of incidents they failed to prevent.

Generating Knowledge Understanding which security controls and procedures effectively reduce risk is a pre-requisite for creating incentives for cybersecurity. In theory, insurers are well-placed to discover this because they collect risk information during underwriting and are notified about any financial losses via the claims process. Over time, insurers could develop statistical evidence about the effectiveness of cyber risk interventions. Thus far, insurers have failed to do so because of data collection and sharing problems. Underwriting data is largely unstructured, such as qualitative answers to questionnaires/video calls [5], and so difficult to analyse with statistical methods. Further, insurers will not share data with each other because claims data is considered to be a competitive advantage [4]. Given the former would be solved by technological underwriting methods and the latter is an incentive problem not easily solved by technical design [6], forensic analysis represents perhaps the area most ripe for innovation.

Cyber insurance exerts considerable influence over how policyholders investigate incidents [7]. Insurers use their market power to drive down the cost of investigations leading to wider use of automated scripts [10]. This motivates research into automated forensics to prevent automation coming at the cost of quality. Further, insurers in the US appoint lawyers at the top of the incident response hierarchy in order to cloak the investigation in attorney-client privilege [10]. The associated legal strategies help prevent investigatory findings (e.g. that the policyholder flaunted basic security procedures) being used by litigants in court cases, but the same strategies also function to distort the documentary record about the cause of security incidents. This may have made sense when the biggest driver of costs was data breach litigation, but not when "litigation rates are around 1% while ransomware payments grew 1000% year-on-year" [10]. Insurers should reflect on who leads incident response, and default to appointing technical leads unless litigation is a very realistic outcome.

Punishing Insecurity The final areas for innovation is the most controversial and also least well understood. Many people believe that cyber insurers ruthlessly avoid paying claims by using exclusions found in the small print. This perception is driven by the media's reporting bias towards disputes like Zurich's court case, in which the insurer claims a war clause was triggered by the NotPetya attack. The media largely ignores the bulk of claims that are paid and that collectively hurt the industry— a survey of 5,600 IT professionals found that "in 98% of incidents, the insurer paid some or all the costs incurred" [11].

The unprofitable loss ratios we discussed earlier are signs that insurers are indeed paying claims [1].

Fundamentally, insurers deal in promises. Excluding claims undermines trust in insurance products, which in turn undermines sales in the future. Thus, insurers are playing an iterated game in which they must protect their own reputation among policyholders and also peers. For example, many within the industry were frustrated that Zurich excluded the NotPetya attack given other insurers had paid out on cases like the Sony hack, which was attributed to North Korea by the FBI. A further consideration is that most cyber insurance is sold via an intermediary, the insurance broker, who controls whether the underwriters get any business [4]. Thus, even if cyber insurance policies include exclusions that would apply in a strict legal sense, in many cases the insurer will not invoke the exclusion in order to protect their reputation and relationship with the broker.

Nevertheless, it is worth asking if it could ever be justified for cyber insurers to exclude a claim. The economic concept of moral hazard suggests not doing so creates perverse incentives by dulling the incentive for firms to secure their networks [6]. This creates a Goldilocks problem as insurers should not seek to exclude all claims, nor should they exclude no claims. Insurers need to find the balance and exclude *the right* claims. Ultimately, insurers need to avoid ambiguous exclusions like "the insured must implement reasonable security" and begin to affirmatively define what basic cyber hygiene consists of and punish those firms who fail to implement it. For example, a large US insurer introduced a Neglected Software Exploit clause in which the policyholder takes on "progressively more of the risk if the vulnerability is not patched at the 46-, 90-, 180-, and 365-day points" [12]. This means that rather than a brittle yes-no decision on whether the policyholder implemented reasonable security, which inevitably leads to costly court battles, the insureds who take longer to apply security patches also pay a higher proportion of claims.

Summary For the first two decades, the cyber insurance market rewarded entrepreneurial insurers who embraced uncertainty while offering innovative insurance products. Supply increased as new carriers launched products seeking to capture a new insurance line. Applicants and brokers began to seek out those underwriters who had the lowest underwriting standards and price, which preventing informed insurers from applying their expertise. Ransomware shattered this equilibrium, creating space for the insurers—both traditional carriers and start-ups—who can accurately price risk and nudge policyholders towards better security.

Going forward cyber insurance providers will thrive by succeeding in: (i) rewarding security; (ii) generating knowledge; and (iii) punishing insecurity. Security will be better assessed and incentivised by partnering with technology providers who have deep access to policyholders' IT architecture. This same information can be linked to claims outcomes in order to generate knowledge about the efficacy of security interventions, although this process is being limited at present by lawyer-led incident response. Finally, insurers need to avoid disputes over ambiguous exclusions like war clauses or *reasonable security*. In-

stead insurers should affirmatively define what cyber hygiene consists of, and exclude claims when it is not followed.

Acknowledgements

This research is supported by REPHRAIN: The National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online (UKRI grant: EP/V011189/1)

References

[1] National Association of Insurance Commissioners Staff. Report on the cybersecurity insurance market. https://content.naic.org/sites/default/files/index-cmte-c-Cyber_Supplement_2020_Report.pdf, 2021. Accessed: 2022-03-11.

[2] Not Unreasonable Podcast. Ty Sagalow on the making of lemonade. https://www.buzzsprout.com/126848/1515319-ty-sagalow-on-the-making-of-lemonade, 2019. Accessed: 2022-03-11.

[3] Sasha Romanosky, Andreas Kuehn, Lillian Ablon, and Therese Jones. Content analysis of cyber insurance policies: How do carriers price cyber risk? *J. of Cybersecurity*, 5(1), 2019.

[4] Daniel W Woods and Tyler Moore. Does insurance have a future in governing cybersecurity? *IEEE Security & Privacy*, 18(1):21–27, 2020.

[5] Jason RC Nurse, Louise Axon, Arnau Erola, Ioannis Agrafiotis, Michael Goldsmith, and Sadie Creese. The data that drives cyber insurance: A study into the underwriting and claims processes. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, pages 1–8. IEEE, 2020.

[6] Ross Anderson. Why information security is hard—An economic perspective. In *Proc. of the Computer Security Applications Conf.*, pages 358–365. IEEE, 2001.

[7] Jamie MacColl, Jason RC Nurse, and James Sullivan. Cyber insurance and the cyber security challenge. *Royal United Services Institute Occasional Paper Series*, 2021. Accessed: 2022-03-11.

[8] Coveware. Ransomware demands continue to rise as data exfiltration becomes common, and maze subdues. https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report, 2020. Accessed: 2022-03-11.

[9] Gordon Lawson. With rising cyber insurance costs and requirements, consider new alternatives to fight ransomware.

https://www.forbes.com/sites/forbesbusinesscouncil/2021/12/22/with-rising-cyber-insurance-costs-and-requirements-consider-new-alternatives-to-fight-ransomware/, 2021. Accessed: 2022-03-11.

[10] Daniel W Woods and Rainer Böhme. Incident response as a lawyers' service. *IEEE Security & Privacy*, 20(2):68–74, 2021.

[11] Sophos. The state of ransomware 2022. https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/, 2022. Accessed: 2022-05-04.

[12] Chubb. Chubb addresses growing cyber risks with a flexible and sustainable approach. https://www.chubb.com/content/dam/chubb-sites/chubb-com/us-en/business-insurance/cyber-enterprise-risk-management-cyber-erm/documents/pdf/2021-10.13_v3_17-01-0295_Widespread_Events_Endorsements.pdf, 2021. Accessed: 2022-03-11.