University of Pennsylvania Carey Law School
Penn Carey Law: Legal Scholarship Repository

Faculty Scholarship at Penn Carey Law

12-4-2022

Insurance and Enterprise: Cyber Insurance for Ransomware

Tom Baker
University of Pennsylvania Carey Law School

Anja Shortland
King's College London

Follow this and additional works at: https://scholarship.law.upenn.edu/faculty_scholarship

 Part of the Insurance Commons, Insurance Law Commons, Internet Law Commons, and the Law and Economics Commons

Recommended Citation
48 Geneva Papers on Risk & Ins. Iss & Prac. (2022)

This Article is brought to you for free and open access by Penn Carey Law: Legal Scholarship Repository. It has been accepted for inclusion in Faculty Scholarship at Penn Carey Law by an authorized administrator of Penn Carey Law: Legal Scholarship Repository. For more information, please contact PennlawIR@law.upenn.edu.

The Geneva Papers on Risk and Insurance - Issues and Practice
https://doi.org/10.1057/s41288-022-00281-7

Insurance and enterprise: cyber insurance for ransomware

Tom Baker[1] · **Anja Shortland**[2]

Received: 8 July 2022 / Accepted: 2 November 2022
© The Author(s) 2022

Abstract

Selling insurance gives insurers an incentive to manage insured risks. The "insurance-as-governance" literature demonstrates that insurers often make insurance conditional on ex ante risk reduction or mitigation. But insurance governs in support of enterprise, not security for its own sake. Tight underwriting inhibits enterprise—not only for insured businesses but also for the business of insurance. This paper highlights ex post loss reduction as a form of insurance-based governance. Drawing on interviews with industry insiders, we explore how insurers addressed the evolving problems of moral hazard, uncertainty and correlated losses since the 1990s. We find that cyber insurance developed sophisticated remedies to contain liabilities and quickly restore affected IT systems, but largely left security decisions to the insured. This facilitated enterprise in the short run but undermined security in the longer term: funding and expediting ransom payments encourages further attacks. As businesses improved their resilience, cybercriminals adapted and ransoms escalated, calling insurability into question. Yet there remains little appetite for imposing restrictive conditionality in this highly competitive market. Instead, insurers have turned to governments to contain criminal threats and cushion catastrophic losses.

Keywords Insurance · Ransomware · Governance

Insurance allows enterprise, and hence multiplies wealth. As a liberator of action….
Ewald 1991.

✉ Tom Baker
tombaker@law.upenn.edu

Anja Shortland
anja.shortland@kcl.ac.uk

[1] University of Pennsylvania Carey Law School, Philadelphia, USA

[2] Kings College London, London, UK

Published online: 04 December 2022

Introduction

One of the world's most politically disruptive cyberattacks started with a compromised password for a dormant employee account, admitting hackers into the network of Colonial Pipeline. When company executives received a ransom demand from DarkSide on 7 May 2021, they decided to shut down operations until a resolution could be found. Five days later, the Eastern seaboard of the US was in political and economic turmoil. As the gasoline price shot up and fuel shortages began to bite, the CEO felt that he had no choice but to pay the attackers USD 4.4 million in Bitcoin to restore operations. The tab for the ransom would be picked up in London: Colonial had bought a USD 15 million cyber insurance policy (Reuters 2021).

Cyber insurance underwriters watched the Colonial ransomware events unfold with mixed emotions. On the one hand, the events provided tremendous publicity for their product. There were seriously bad, foreign actors, widespread and visible consequences, and insurance played a key role in the response. (As a bonus, the FBI later recovered about half of the Bitcoin because of a mistake by the extortionists.) On the other hand, the publicity could lend support to the growing criticism that cyber insurance normalised a deeply troubling and immoral ransom process (Dudley 2019).

These mixed responses to the Colonial ransomware event illustrate a tension between security and enterprise that appears whenever insurance engages with crime. Is insurance to be a liberator of action that allows enterprise, in this case by making the ransom payment that brought the pipeline back online sooner than would have been possible without the decryption key the ransom purchased? Or is it to be a guarantor of security that, in this case, failed twice: once by failing to persuade or compel Colonial to adopt whatever security measure would have prevented the hacking in the first place, and then by paying a ransom that likely encouraged the proliferation of ransomware?

To date, the insurance-as-governance literature has focused primarily on the security side of this tension, to the neglect of enterprise. Yes, steps that insurers take to manage moral hazard, address adverse selection or contain catastrophic risk can and do function as a kind of governance or regulation (Heimer 1985; Ericson and Doyle 2004; Ben Shahar and Logue 2012; Abraham and Schwarcz 2023). And, yes, that governance can promote security and thereby prevent loss. But that security is a byproduct, not the objective, of insurance. Everybody involved cares primarily about their enterprise: namely, the productive things that they want to do—their business—and that would not be possible to do if the maximum-security position were mandatory. It's not that they don't care about security or insurance. They do care: but as means, not ends. Even the insurers, for whom insurance is their enterprise.

The neglect of insurers' role in facilitating enterprise leads to, or perhaps follows from, an understanding of the "governance" in insurance-as-governance as efforts to encourage risk reduction and loss mitigation. This is understandable, as the pioneering insurance-as-governance researchers were working against habits of mind that made it hard to see the governance in insurance relationships. According to this mindset, private insurance was about risk transfer, spreading and distribution, not

governance (Ewald 2020/1986). The pioneering sociologists were working against the notion that governance is done in and by the state (Heimer 1985; O'Malley 1991), and the pioneering economists were working against the notion that insurers were passive loss spreaders (Arrow 1963; Shavell 1982). To expand the existing habits of mind, it was easiest for them to point to situations in which insurers were telling people what to do: no burglar alarm, no home insurance (O'Malley 1991); a "seaworthy" vessel, or no marine insurance (Heimer 1985); no keg parties, or no insurance for fraternities (Simon 1994). In other words, if the objective was to demonstrate that insurers have an incentive to govern (e.g. Shavell 1982) or to demonstrate that insurers in fact do govern (e.g. Heimer 1985), then it made sense to focus on risk reduction and loss mitigation.

But there is also governance involved in helping people to do what they want—such as creating norms, protocols or structures to limit the cost of resolving insured events after they have occurred. This understanding of the governance role of private insurance has a longer pedigree than the more restrictive understanding that some derive from the insurance-as-governance literature (e.g. Abraham and Schwarcz 2023; Avraham and Porat 2022). Consider the preamble to the English Insurance Act of 1601.

> Whereas it ever hathe bene the Policie of this Realme by all good means to comforte and encourage the Merchante, thereby to advance and increase the generall wealthe of the Realme, … And whereas it hathe been tyme out of mind an usage amongste Merchantes, both of this Realme and of forraine Nacyons, when they make any greate adventure (speciallie into remote partes) to give some consideracion of Money to other peons (which comonlie are in noe small number), to have from them assurance made of their Goodes Merchandizes Ships and Things adventured, … by meanes of whiche Policies of Assurance it comethe to passe, upon the losse or perishinge of any Shippe there followethe not the undoing of any Man, but the losse lighteth rather easilie upon many, than heavilie upon fewe, and rather upon those that adventure not than those that doe adventure, whereby all Merchantes, speciallie the younger sorte, are allured to venture more willinglie and more freelie ….

Specifically, the act created a new standing tribunal to adjudicate marine insurance disputes "… in a briefe and summarie course as to their discretion shall seem meete without formalieties of pleadings or proceedings" (cited in Holdsworth 1917, p. 103). This reduced the cost of providing insurance and allowed merchants "… the better followe theire trades without encomberounce or molestinge the one the other by suites at lawe, bothe to the hinderance of traffick and of her Majesty's customes" (cited in Holdsworth 1917, p. 99). So, here we have the sovereign explicitly promoting enterprise by helping insurers create more efficient (self-) governance structures.

At this time, the significant insured threats to international trade included crime, piracy, hostage-taking and demands for ransom. In this study, we examine how insurance engages with the online version of kidnap for ransom as a case study in the governance of crime and insurance-as-governance. Drawing on in-depth interviews with industry insiders and participation in industry events (see "Appendix" for

a listing), we observe governance by insurers that is context specific. In the US, specialty-lines liability insurers dominate the cyber insurance market. They have largely (and rationally) focused on the litigation risk that their customers face, creating a governance architecture focused on reducing or hiding liability rather than reducing crime. By contrast, in Europe, kidnap and ransom (K&R) insurers focused on containing criminal extortion. With the recent rise of ransomware, those two approaches may converge, perhaps with the help of states.

The primary objective of this paper is to bring a renewed focus to insurers' role in facilitating enterprise into insurance-as-governance research. Building on prior work (Shortland 2019, 2021; Baker and Shortland 2022), we chart the evolutionary fashion in which insurance engaged with a dynamic criminal threat in a highly competitive market. We identify and analyse the techniques that insurers used to limit losses and manage uncertainty, extending prior research on insurance as an "uncertain business" (Ericson and Doyle 2004; Baker 2021). We add a new, comparative dimension to prior work on the history of cyber insurance (e.g. Wolff 2022) by highlighting an approach taken earlier in London that is worth considering today. Our conclusions promote more realistic expectations about the type and extent of governance that can be expected from cyber and other kinds of insurance.

The paper is structured as follows. The next section discusses the challenges posed by ransomware, the ways in which insurers can shape risks to maintain insurability and our research method. The subsequent section offers a rich description of the origins of cyber insurance in which the threat of extortive cybercrime played only a minor role. We then explore the response of cyber insurance to the emergence and development of ever more sophisticated ransomware. In the penultimate section, we analyse how insurance markets balanced the competing interests of security and enterprise in this ever-changing threat environment. The final section concludes with some policy implications.

Insurance and governance

For insurance to govern within a social field, there must be insurers willing to provide financial protection against risks present in that field. We cannot here provide a ground-up description of the conditions necessary for insurance, among other reasons because insurability has an ineluctably subjective element. Nothing is insurable until there are insurers willing to provide the insurance, and if there are such insurers, those risks are insurable, even if some actuaries or economists (correctly) predict that the insurers will eventually become insolvent paying the losses (Karten 1997). Conversely, risks are not insurable if there are no insurers willing to provide the insurance, even if some actuaries or economists have prize-worthy models demonstrating that the risks should be insurable. Notably, all real-world insurance is partial, so if insurers are willing to provide only partial insurance that doesn't make a risk uninsurable. Thus, ransomware is insurable, at least today, and there is a large and growing insurance market dedicated to the proposition that it will remain insurable, even if some of the participants in that market believe that government action will be needed (Pal et al. 2021).

We focus here on three aspects of insurance for ransomware that are widely considered to pose insurability problems: moral hazard, uncertainty and catastrophic risk. Moral hazard, or the reactive nature of insured risk, is present to varying degrees whenever there is insurance (Baker 1995), but it presents special difficulties in the context of crime. Crime requires human actors, who are understood to act with intention and, thus have the potential to react to anything that changes the payoffs from their actions (Heimer 1985). Moreover, the criminals are strangers to—but potentially knowledgeable about—the insurance contract, presenting a third-party moral hazard that is notoriously difficult to control (Parchomovsky and Siegelman 2022).

Uncertainty—in the sense meant by Knight (1921), who distinguished it from risk—is not connected in any special way to crime. Indeed, discovering the statistical regularities of crime, thereby bringing it within the realm of risk, was among the earliest accomplishments of the social sciences (Daston 1987). Ransomware and other cybercrime losses may one day prove to observe similarly predictable patterns but, at least for now, they are believed to be unusually uncertain (Guidewire 2020). And uncertainty poses a challenge whenever insurers charge fixed prices today for protection against future losses (Arrow 1963; Baker 2002, Baker 2021). Similarly, catastrophic (correlated) risk is not a specific feature of crime, but correlation does present special concern in the cyber context. Cybercrime is understood to present new potential for correlation and, as a result, a radically increased scale of loss, perhaps exceeding that of its close cousin, terrorism (Abraham and Schwarcz 2021; Pal et al. 2021).

Extending insurance gives insurers a stake in managing the risks insured, including the attendant moral hazard, potential for correlation and uncertainty. That simple insight lies at the core of much of the insurance-as-governance literature, especially the contributions by rational choice theorists (e.g. Heimer 1985). The fact that insurers have a stake, however, does not tell us what they do about that stake, including whether they choose to do anything at all. That requires investigation. Qualitative research has revealed many things that insurers do in various contexts to manage risks, though certainly not all are done in every case (e.g. Heimer 1985; Baker and Griffith 2010; Shortland 2019). The tools that insurers use to manage moral hazard, uncertainty and catastrophic risk include the following:

- Scrutinising prospective insureds to weed out those they are unwilling to insure, and to identify those they are willing (at least partially) to insure.
- Charging different prices for insureds that pose different levels of risk.
- Excluding or limiting coverage for risks that pose an unacceptably high degree of moral hazard, uncertainty or potential for correlation.
- Imposing rules of conduct designed to reduce the likelihood or size of insured losses.
- Selling insurance for a series of short time periods, rather than one long period, preserving the ability to examine the risks anew each time and to change the price and other terms, or to refuse to renew at all.
- Paying only up to a fixed amount for a covered loss (even if the loss to the policyholder is much larger), thereby limiting their exposure to any individual loss.

Insurance policies also often limit the insurer's total exposure under the policy, regardless of the number of losses.
- Creating systems for managing losses adapted to the (first and third party) moral hazard present in the loss.
- Monitoring risks across their portfolio to identify trends and the possibility for correlation, adjusting sales, renewals and reserves in response.

Many of these tools have the potential to function as forms of governance. In this paper we study whether and how they were used in cyber and ransomware insurance over time and in different jurisdictions. Notably, ransomware insurance was never designed from scratch but was adapted from and built into existing cyber (or other) insurance policies, which in turn were shaped by national laws. As criminal innovations turned ransomware from a minor nuisance into a serious threat to profitability, insurers had to innovate against the background of a highly competitive market for cyber insurance. Insurers were thus guided in their choices on how to manage risks by path dependence and fierce (evolutionary) competition. Overall, we observe more innovation on managing losses ex post than on the risk reduction measures that have traditionally been the focus of the insurance-as-governance literature.

To explore the history of cyber and ransomware insurance, we conducted 25 in-depth, unscripted interviews with senior practitioners in insurance, the law, security and policy research in Europe and the US. Some of our interviewees engaged in long-running conversations with us as the project took shape from Q4 2019 to Q2 2022 and provided feedback on earlier drafts of the paper. We started with contacts from our previous research, who introduced us to further colleagues. We made additional contacts in four conferences and workshops (see "Appendices 1 and 2" for details). Several of our interviewees had decades of experience in their respective fields and some shared their early (promotional) material about cyber insurance with us. Others had entered the market recently with innovative insurance, pre- or post-breach products. Our interviewees spoke on the condition of anonymity, while workshops were conducted under Chatham House Rule. We have therefore cited academic articles and contemporary trade and media sources whenever possible to evidence the information given to us.

Cyber insurance: origins and overview

When we interviewed industry experts about the history of cyber insurance (and examined the insurance trade literature as a check on their recollections), four high level generalisations emerged. First, there has been a long-term trend of insurers shifting coverage for cyber risks out of their general-purpose liability and property insurance policies and putting that coverage into specialised cyber insurance policies (with a notable exception for very high value commercial property insurance policies, which often provide some data destruction and breach coverage, subject to comparatively low sublimits).

Second, these cyber insurance policies consist of a set of defined coverages, with relatively low limits (compared to typical limits for general-purpose property and

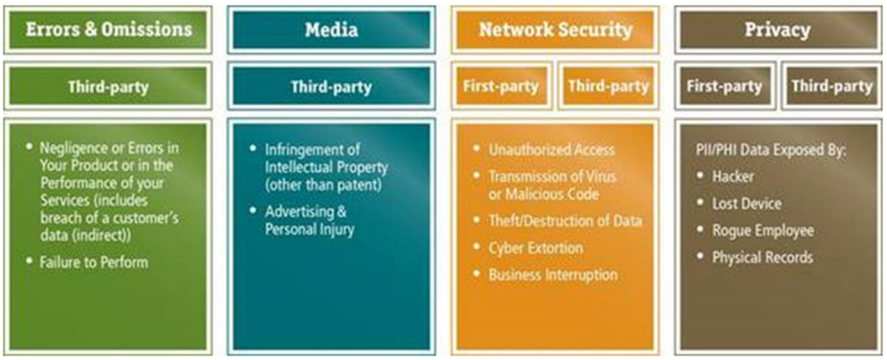

Fig. 1 Categories of coverage provide by cyber insurance policies

liability insurance), targeted at specific risks. These defined coverages are illustrated in Fig. 1, which was taken (with permission) from the website of one of the earliest cyber insurance promoters in the U.S., Peter Taffae (see also Romanosky et al. 2019). The top-level bar names the coverage. The second level bar identifies whether the coverage is "first party" (meaning it pays for losses to the policyholder's business) or "third party" (meaning it pays the policyholders' liabilities for the losses of third parties such as customers, and the costs of defending against those liabilities) or both. The bottom bar identifies the kinds of events the coverage is designed to protect against.

Third, as Fig. 1 illustrates, protection against third-party risks is the centre of gravity of cyber insurance. Although the policies include first-party coverage, much of that coverage pays for the cost of providing notices and services to customers or other third parties and for restoring services that the insured business needs to avoid incurring liabilities. For example, the first-party losses under the privacy coverage consist largely of the costs of identifying whose data were compromised in a breach event and providing notification and privacy monitoring services to those people, so that the business does not incur financial liabilities as a result. The same is true for the first-party network security coverage. A significant share of the losses incurred in recovering from a network security breach—including a ransomware event—can be understood as not just the costs of keeping the insured business going but also the costs of preventing or mitigating the business's liabilities to other people because of the network security breach. This is especially true when the breach is part of a modern, "double extortion" ransomware attack, which we discuss later on.

Finally, selling the set of narrowly defined coverages shown above helps insurers manage uncertainty. Although market participants typically refer to their policies as "cyber insurance policies", the policies do not provide coverage for *everything* cyber. Instead, they provide the coverage agreed in the contract, and only for losses up to specified amounts. Insurers' exposure is therefore capped by kind of loss, both on a per policyholder and overall basis. In addition, the policies provide coverage only for 1 year, typically on what is referred to as a "claims made" basis—meaning that the insurer must pay only those claims made during the policy period or very

shortly afterwards. As a result, insurers know their cyber losses relatively quickly, and they can reprice and revise the coverage terms every year. Moreover, cyber insurance represents only a small part of the business of leading cyber insurers like Chubb, AIG and underwriters at Lloyd's, providing plenty of opportunities for cross subsidies if the worst were to happen to their cyber insurance book (Baker 2021). As a result, despite insurers' concern about the uncertainty involved in extending insurance against new and dynamic criminal risks, cyber insurance was and remains an expanding and—for most insurers—a profitable business.

Multiple beginnings…

Cyber insurance dates to the mid to late 1990s, when entrepreneurially minded underwriters and brokers identified several new risks created by the rise of the internet for which customers' existing policies did not explicitly provide coverage. There were (at least) four simultaneous but initially separate strands of early entrepreneurial activity, based on concerns raised in different branches of insurance.

First, media liability underwriters realised that by advertising and selling on the internet, thousands of businesses became publishers, potentially subject to liabilities that were not covered by their general liability insurance but by media liability insurance. These underwriters developed new insurance products like Chubb's Safety' Net, which was a modified media liability policy marketed to protect Main Street businesses from publisher-type liabilities that were not covered by their existing insurance (Baker 2019).

Second, underwriters selling errors and omissions insurance to technology companies realised that traditional miscellaneous professional liability insurance policy forms were not well adapted to software businesses. Software increasingly migrated towards a software as a service (SAAS) model that kept the software companies' networks connected to their customers. Those businesses needed coverage not just against negligence claims, but also against losses that they could suffer, *despite taking reasonable efforts*, because of hackers, malware, denial of service attacks, cyber extortion and other risks that were emerging on the internet. These technology insurance underwriters developed new insurance products like CIGNA's DataGuard policy, which combined "computer crime insurance" with "comprehensive software insurance".

Third, as Josephine Wolff has described, brokers focusing on technology companies realised that the growth of online commerce was creating new privacy risks for companies collecting and storing customer credit card numbers and other information (Wolff 2022). These, brokers persuaded insurance companies to develop new products like AIG's Internet Security Liability policy, which provide liability coverage for the consequences of stolen credit card numbers. Liability risks escalated when the US introduced legislation to protect personal information held by healthcare providers (1996), financial service providers (from 1999) and other companies holding client information (from 2002). With tightening compliance requirements and the threat of punitive fines, liability insurance became a necessity for an ever-wider group of enterprises.

Fourth, "special risk" insurers in the Lloyd's market—both British and American—offered cyber insurance based on their long-standing experience with K&R insurance. In the late 1970s, Lloyd's insurers had created an innovative protocol for reducing the risk of and mitigating losses from extortion (Shortland 2017). Detailed ex ante security advice, hiding the insurance relationship, and dedicated "crisis responders" to resolve incidents became integral to Lloyd's K&R insurance. The product focuses on containing third-party moral hazard. Professional negotiators take charge of the ransoming: encouraging kidnappers to keep hostages safe as they patiently barter down the ransom (and collect information for law enforcement). Most kidnappers thus make little or no profit considering the risk and cost of acquiring, securing and keeping hostages alive (Shortland 2019). Over time, this successful protocol was adapted to other threat extortions, such as product contamination. The K&R handbook was also seen as a natural fit for extortive cybercrime. Customers were offered "cyber extensions" to their K&R insurance and crisis responders were tasked with handling cyber extortion incidents. Insurance policies such as Lloyd's e-Commerce and Hiscox' Hacker Insurance explicitly covered the cost of "services to mitigate 1st party losses" (Majuca et al. 2006; Rossi 2001).

The shake-out period

Although insurers initially developed cyber policies in different "silos", firms wanted to reduce the administrative burden of covering the various first- and third-party risks related to their online business through multiple standalone policies. Brokers and underwriters therefore developed amalgamated "cyber" products tailored to the needs of different industries and countries (Rossi 2000).

Some of the insurance lines discussed above are obviously complementary. However, the liability-centric and the K&R approach to extortive cybercrime were not. In the US, obligations for breach notification are triggered when a company finds out what customer data have been compromised. Firms can reduce liability risk by resolving breaches before they become public and conducting the transaction under client-attorney privilege. By not fully investigating the precise nature of the breach, first- and third-party costs are minimised and reputational damage avoided. By contrast, the K&R protocol had the potential to inflate resolution costs—especially when hackers only demanded ransoms in the hundreds, thousands or tens of thousands of dollars (Waddell 2016). Interrupting businesses to barter down perfectly affordable ransoms while risking a privacy lawsuit and punitive fines was far costlier than any savings that could be achieved through instilling ransom discipline.

After a shake-out period that can be observed in the annual "Cyber Risk Market Surveys" released by Richard Betterley beginning in June 2001, the combined products won out in the US market (Betterley 2001–2010). The triumph of the liability-centred approach is best illustrated by the decision of Chubb—a market leader in K&R insurance—to join with the rest of the cyber insurance market in including cyber extortion coverage in its cyber insurance policy in 2009, rather than requiring

policyholders to purchase separate K&R cover (Betterley 2008, 2009).[1] In Europe, where data protection concerns were muted until the adoption of the GDPR legislation of 2018, cyber extensions to Lloyd's K&R insurance continued to exist until around 2019, as a cheap add-on to K&R policies.

Mitigating cyber losses

As cyber insurance was developed, the most salient threat was the theft of personally identifiable information. The primary risk to the insured businesses was liability to third parties (e.g. Betterley 2005–2010). The most important insurable losses were breach response costs and, when data were destroyed (a less frequent occurrence), the costs of reconstruction. Insurers found that many insureds handled this process badly: inadvertently amplifying their liabilities and overpaying vendors. They realised that they could make significant cost savings by coaching the insured through the breach response process. Breach victims required legal advice to minimise liability risk, logistical help with breach notification, IT recovery services, identity theft monitoring services and public relations advice. Incidence response firms formed to offer bespoke and competitive post-breach packages combining these services. Privacy lawyers usually lead and coordinate the response: not because they necessarily have the relevant expertise, but because client-attorney privilege reduces the probability of breach victims getting drawn into expensive lawsuits (Woods and Böhme 2021). Insurers soon saw the benefits of outsourcing breach response to pre-selected, reputable, "authorised" providers, who worked hard to deliver good service at competitive prices. This absolved the insured of the need to (slowly and expensively) curate their own response and reduced hold-ups and overall resolution costs (Woods and Böhme 2021). Connecting customers to networks of reputable service providers became a major selling point for cyber insurance.

By contrast, insurers didn't require policyholders to do much in terms of loss prevention. Early on, some cyber insurers tried to understand (and improve) their customers' security stance. They undertook expensive security assessments in the underwriting process, but soon found that the payoffs did not justify the effort. Customers resisted products requiring lengthy and intrusive assessments and security measures that interfered with efficient communication and their ability to conduct business. Additionally, establishing whether customers had correctly followed the specified protocols before paying a claim would have been costly and potentially damaging to the insurance relationship. Security assessments were abandoned when insurers couldn't demonstrate the value in underwriting results: Betterley (2001–2004) shows an initial increase followed by a rapid decline in insurers that required assessments.

Thus, most product innovations in cyber insurance focused on damage mitigation. This situation disappointed security professionals and insurance-as-governance researchers (Cunningham and Talesh 2021), because they were looking for

[1] Up until 2008, Betterley reports that Chubb excluded extortion cover from its data theft policy; from 2009, it is included.

ex ante security governance—not for institutions that mitigated losses ex post. Yet cyber insurance was profitable without hands-on security governance: offering partial insurance was sufficient to encourage customers to limit their exposure. The market was growing fast, and insurers' underwriting results were favourable. Loss mitigation, short policy periods, low policy limits, and rapid repricing protected cyber insurers from poor underwriting results. The insurers' complaints, to the extent they had them, were that buyers were not recognising the value of cyber insurance as quickly as insurers would like (Betterley 2005) and that policyholders were attempting to recover for cyber losses under their general-purpose property and liability insurance policies (Yost et al. 2001). However, market practices were called into question by the explosion of ransomware attacks and the escalation of ransom demands from 2016 onwards.

The evolution of ransomware and cyber insurance

Ransomware is a type of malware that encrypts and thereby prevents victims from accessing data on their system until a ransom is paid (Richardson and North 2017).[2] Ransomware is a long-running phenomenon that increased in sophistication over a period of more than 30 years. Until 2013, cyber extortion scarcely registered as a problem for insurers. Subsequently, potential victims and/or insurers responded to changes in the threat level with a combination of measures to lower the success rate of breaches, increase resilience against extortionist demands, facilitate smooth resolutions, reduce the collateral damage from attacks and lobby for improved law enforcement.

The first known incident of what we now call ransomware dates to 1989 (Wilding 1990). The so-called AIDS Trojan scrambled the computers of thousands of medical researchers who had loaded a programme purporting to help them determine patient risks. On the 90th restart, the Trojan encrypted their data and demanded a ransom of USD 189. However, it was cumbersome to make the payment: victims had to send cheques or money orders to a PO Box in Panama to obtain a decryption key. Many avoided making a payment when security experts cracked the code (Waddell 2016). Subsequent extortionists tried to arrange payment using gift and phone cards or premium telephone lines where victims were charged by the minute for calling designated numbers. The risk of being tracked by law enforcement inherent in such low-tech and cumbersome payment mechanisms kept ransoms low. Thus, for many years, the fear of cyber extortion had a positive impact on insurance: creating higher premium income than what (carefully worded) insurance policies paid out.

[2] There are other forms of cyber extortion beyond the scope of this paper. In extortive (distributed) denial of service attacks, criminals threaten to overwhelm the victim's server with malicious traffic to make it impossible to conduct legitimate business. Extortionists may also threaten to leak personal data, sensitive images or business-critical information obtained by theft, phishing or intercepted communications.

Although two computer scientists published a paper in 1996 that predicted the marriage of malware and strong encryption that characterises contemporary ransomware (Young and Yung 1996), cyber extortion did not emerge as a notable threat until at least 2005, or even later (compare Beamon et al. 2021 with Hampton and Baig 2015). Profit-oriented cyber hackers focused on stealing and selling data, such as credit card numbers, or organising botnets that could be leased to others seeking to launch denial of service attacks or other activities for which such networks were useful (Hampton and Baig 2015; Lusthaus 2018). The CryptoLocker ransomware attack in 2013 is credited as a milestone event that brought ransomware to widespread attention (Kharraz et al. 2015).

This timing is important because it means that the cyberinsurance market and its incident response architecture had developed before ransomware emerged as a significant threat. Privacy lawyers routinely handled cyber claims but had little or no experience of responding to extortion, ransom bargaining or facilitating transactions with criminal entities. Client-attorney privilege hides valuable information about modes of attack, client vulnerability and negotiation tactics from other stakeholders—including law enforcement (Schwarcz et al. 2023). This approach exacerbated third-party moral hazard: when extortionists meet no resistance to their demands, they tend to escalate their activities and raise prices—if they can.

Our interviewees highlighted two key developments at the end of the first decade of the twenty-first century to explain the shift in criminal focus from stealing data to ransomware. First, the market value of stolen credit cards collapsed when the highly successful Zeus Trojan led to an oversupply of financial credentials on the dark web (Krebs 2010). This led criminal groups to look elsewhere for more profitable activities. Second, Bitcoin and other cryptocurrencies emerged as a payment mechanism that would make ransomware into a highly successful criminal business model (Kharraz et al. 2015; Popper 2015). Hampton and Baig (2015) identify the following three technologies as core to a ransomware business:

- "Strong, reversible encryption to lock up a user's files",
- "A system for anonymously communicat[ing] keys and decryption tools" and
- "An untraceable way to pay the ransom".

Encryption had developed earlier to secure data from theft and protect privacy (Froomkin 1995), and Young and Yung had already predicted back in 1996 that it could be linked to malware. Anonymous communication systems had also developed earlier, among other reasons to facilitate the sale of stolen data (Lusthaus 2018). When Bitcoin was released in 2008 and proven to have a market value a short time after (Popper 2015), extortionists finally had a manageable way to be paid without risking exposure or being shut down. Although Bitcoin's public ledger means that Bitcoin payments are traceable to at least some degree, the payments have to date remained adequately anonymous if the recipient is careful not to leave a trail that allows their identity to be linked to the Bitcoin address (Paquet-Clouston et al 2018). Moreover, many ransomware operators work out of jurisdictions that do

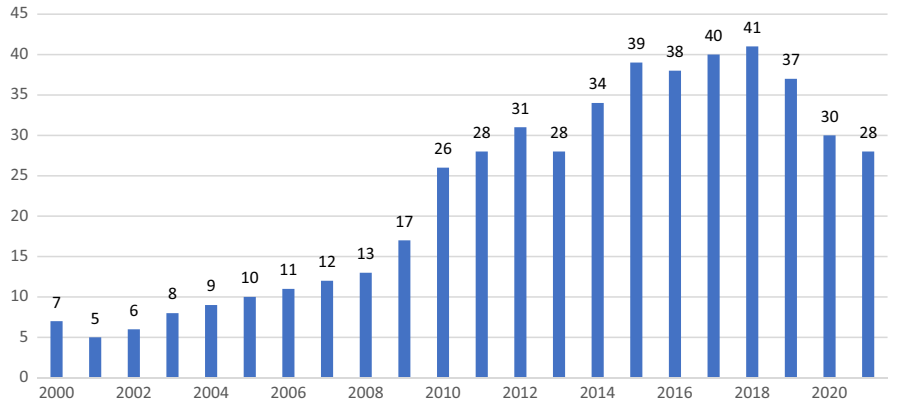

Fig. 2 Number of insurers in the cyber market (Betterley reports 2000–2021)

not cooperate with international cybercrime control efforts, reducing the payoff from law enforcement efforts to make that link.[3]

First-generation RaaS: 2016–2018

Once the core technologies were in place, ransomware could be scaled up. From 2016, criminal software engineers developed the ransomware-as-a-service (RaaS) business model that allowed them to outsource the time consuming "breaking and entering" part of the cyber extortion to "affiliates" who shared the proceeds with the coder (Lusthaus 2018). Initially, both threats and resolutions were largely automated: victims would face a standard ransom demand for a few hundred dollars, a test decryption portal on TOR and a button to make the payment, which automatically released the decryption tool (Coveware 2022a). As a result, attacks not only became more frequent but more disruptive. The coders had limited or no control over sloppy affiliates or the "aftercare" they provided. Most affiliates did not have the technical know-how to help victims restore their systems. If the automated decryption failed, affiliates (who had already made their profit) generally left victims to their own devices, effectively turning ransomware into data-wiping malware.

Figure 2 shows the number of companies that offered cyber insurance and disseminated their product in the industry surveys in the annual Betterley Reports over time. RaaS arrived during a period of tough competition for market share and very few insurers chose to market products with stringent security conditionality. Instead, they once again focused on loss mitigation. Ransoms were only in the thousands of dollar range, but total recovery costs could easily be orders of magnitude larger. For

[3] The recent, high-profile arrest of the American couple that allegedly hold the keys to Bitcoin stolen in the 2016 Bitfinex heist illustrates this dynamic: the heist was large enough to draw law enforcement attention (over USD 3 billion), they left some (faint) traces, and they remained in New York long enough for law enforcement to find and follow those traces (Watkins & Weiser 2022).

example, the Lansing Board of Water and Light paid a USD 25,000 ransom in 2016, but the final bill for response and recovery came to USD 2.4 million. This pattern of losses encouraged insurers to improve resolution and recovery protocols rather than focusing on ransom discipline.

Breach victims turned to IT firms to help them through different aspects of the ransomware process: identifying what data had been compromised, investigating whether it could be unencrypted or restored from backup without a ransom payment, or—if necessary—pay a ransom to decrypt the data and restore the files. Finding support was not always easy, prices could be steep, and the quality of services was opaque (Coveware 2018a). Many decryption and recovery tools—even from major IT firms—proved ineffective or only partially effective in restoring compromised data (Filiz et al. 2021). "Ransomware payment mills"—associates of hackers posing as legitimate ransomware recovery firms—advertised their services alongside reputable providers. Due to their links with the underworld, they could provide victims with priority support—but for inflated fees and at the risk of breaking the law by paying sanctioned criminal groups (Coveware 2018b).

Insurers thus had a strong incentive to identify and connect their clients to effective ransomware resolution services and integrate these into their existing cyber incidence response architecture. Almost everyone in the market prized fast and reliable resolution, which meant paying ransoms when this was the lowest cost option. Yet, rather than increasing security, this form of insurance-as-governance—a breach response infrastructure that effectively rewarded high-quality ransomware—increased *insecurity* when criminals responded to these incentives.

Second-generation RaaS: 2018–2019

As more criminal gangs entered the ransomware business, IT firms and breach responders developed new lines of informal communication. Online platforms shared information on which extortionists could be trusted to provide a reliable decryption service after receiving the ransom payment and expose those who did not (Coveware 2022a; Woods and Böhme 2021).[4] Off-the-shelf decryption keys that worked for multiple victims were shared, occasionally making free recoveries possible.[5] This created the incentive for criminals to develop more advanced cryptography and reputations for smooth decryption services. Criminals worked on making the decryption process as painless as possible, with some ransomware brands priding themselves on being impressively responsive to customer concerns (Coveware 2019). However, doing so raised the cost of committing ransomware attacks, and hackers innovated to make successful breaches more profitable.

Once criminals were inside a company's system, they could research the victim's ability to pay—sometimes even by locating the company's cyber insurance certificate—and hence engage in price discrimination. Instead of an automated demand

[4] See also the Ransomware Recovery blog published by Coveware at https://www.coveware.com/ransomware-blog.

[5] See for example the website of the "No More Ransom" organisation https://www.nomoreransom.org.

and payment system, the criminal software developers provided darknet "chat" platforms that could handle multiple extortions at a time (Coveware 2022a). When hackers breach critical infrastructures (healthcare providers, utilities or local authorities) ransomware works like traditional hostage-taking. With lives at risk and municipalities unable to run services, communicate or process payments, ransoms escalated into the millions. Sometimes ransom demands were excessive and unaffordable—especially for payments processing firms. Victims would have to explain to sceptical hackers that turnover does not equal profit and the meaning of a "ransomware sublimit" in an insurance contract.

Communicating with criminal enterprises on the darknet, bartering over ransoms, and obtaining and paying ransoms in cryptocurrency were also soon offered as expert services—either separately or in a ransomware-settlement-as-a-service package. Law firms coordinating breach response continued to help victims cloak all these activities within legally protected communications and documents, to reduce the chance that a target's customers, shareholders or other third parties would be able to reveal or criticise a ransomware event (Woods and Böhme 2021; Schwarcz et al. 2023). Finally, for those who had bought cyber insurance, insurers reimbursed the ransom payments and paid for the post-breach services.

As any rational choice theorist would predict, the success of sophisticated ransomware led to an increase in both activity and ransom demands and, at the same time, helped to fuel the market for cyber insurance. Current and prospective policyholders learned that insurers would not just reimburse the ransoms, they would also connect targeted businesses with breach response experts who knew how to (a) pay the ransoms, (b) manage the attack so that the business could get back online and (c) become less vulnerable and more resilient the next time. Paying for these breach responses services allowed insurers to provide significant value to their customers and thereby participate in the fastest growing sector of the commercial insurance market, without exposing their balance sheets to unacceptable levels of uncertainty. Because the insurers were buying in bulk, they paid less for these services than policyholders would themselves, and they could quickly connect their customers with services they desperately needed.

In most cases, even the newly increased ransoms were modest in amount compared to both the value of the data to the business and traditional property and liability insurance losses. As a result, quick payment of ransoms still made sense for both the business and the insurer. Premia remained manageable for the policyholder and profitable for insurers. Moreover, because the amount of cyber extortion coverage in any individual policy was capped at comparatively low levels, insurers were protected from extreme risks. Finally, because cyber insurance policies are repriced every year, insurers could adjust premiums on a regular basis in response to increases in the frequency or severity of ransomware attacks (which they closely track with the help of vendors), further reducing the likelihood of underwriting losses. Carefully managed cyber books thus continued to produce mostly favourable results (Betterley 2018). The big issues for insurers in the period to late 2018 remained motivating more businesses to buy cyber policies and avoiding coverage for cyber losses under traditional liability/property policies, as can be seen in the litigation brought by Mondelez and Merck seeking coverage under their property

insurance policies for the NotPetya malware attack, with more than USD 1 billion at stake for Merck and more than USD 100 million for Mondelez (Voreacos et al. 2019).

Third-generation RaaS and "systemic risks" (2019 onwards)

As ransomware became ever more prominent, firms engaged in greater efforts to protect themselves through measures beyond simply purchasing cyber insurance. Whatever one may think about the impact of insurance on incentives more generally, there is no such thing as complete insurance against a ransomware attack. The disruption extends beyond the costs of vendors and ransoms, and even beyond the business interruption losses that some insurers are willing to insure. Whether for this reason or others, businesses began to take steps to become less vulnerable to ransomware attacks and more resilient in response to attacks, for example by employing multifactor authentication and by regularly updating and testing offline backups. As a result, low-tech attacks became preventable, and in case of successful breaches, some victims could safely refuse to pay ransoms, frustrating attackers who had spent time and money launching the ransomware attack (Fuentes et al. 2021).

The third-generation ransomware attack therefore involves what computer security professionals refer to as "double extortion" (Fuentes et al. 2021). In this strategy, the attackers raise reputational and liability risks for the company (and their insurer). They invest even more time inside the target's servers to identify and exfiltrate the data that the target would least like to become public and only then launch the ransomware that encrypts the target's data. As in the second-generation attacks, criminals use the information gained to tailor the size of the ransom. If the target refuses to pay or stalls, the attacker threatens to release the data. If it becomes public that personally identifiable data have been compromised, reputational costs and third-party damages massively increase the cost of resolution—especially for companies like healthcare and education providers that routinely handle sensitive personal information. Hackers found that data leaked on darknet forums was quickly picked up by bloggers and journalists ready to sensationalise their "scoop" (Coveware 2022a). Alternatively, attackers could contact the company's customers or suppliers using their stolen contact details to intensify the pressure to pay the ransom. Once leaked, stolen data no longer serve as a bargaining tool, but selective leaking and building a reputation for following through on threats can be highly successful in persuading companies to pay (Krebs 2022). Figure 3 shows data from a breach responder showing the rapid acceleration of ransom payments from 2019.

With the rise of the double extortion strategy, cyber insurers and their insured businesses find themselves in a Catch 22. Minimising liability risk through quick, private payments increases ransom risk, as the recent, rapid growth of highly sophisticated ransomware attacks reveals. At the same time, minimising ransom risk by careful investigation and refusal to pay high ransoms increases the liability risk from the release of sensitive data. There is a growing concern that third-party moral hazard is getting out of hand (Baker and Shortland 2022). Moreover, with ransomware gangs regularly disbanding and reforming (Lusthaus 2018), nobody can rest assured

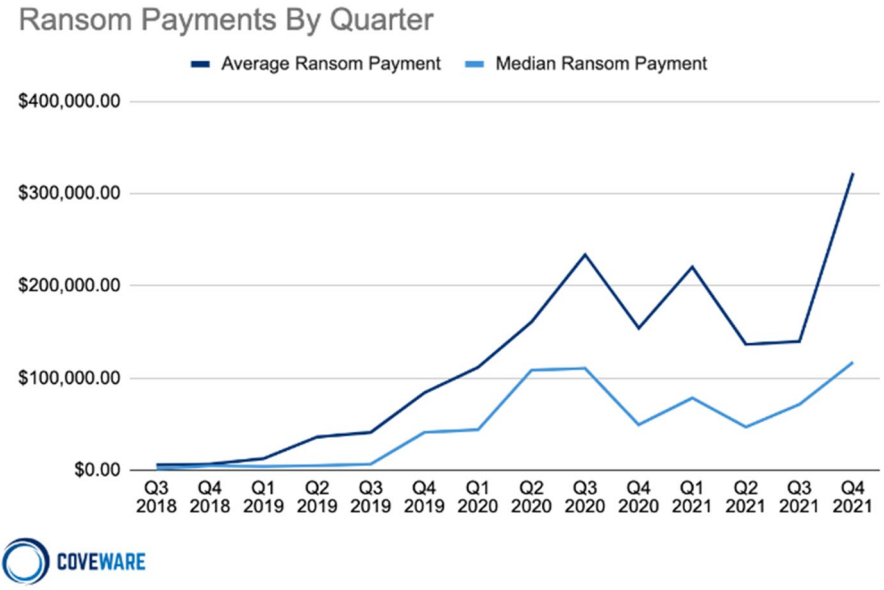

Fig. 3 Ransom payments by quarter from Coveware (2022b)

that exfiltrated data are not copied and sold—or that they might be sold at a later stage.

A further dangerous development took place in 2020, when hackers began to target cloud storage, software supply chains and managed service providers (MSPs) to deploy malicious software. MSPs have trusted access to hundreds or even thousands of clients' systems to provide updates, patches, alerts and remote computing support. The 2021 attack on Kaseya systems affected up to 1500 enterprises while 18,000 customers of SolarWinds installed corrupted updates in 2020 that left them open to future attacks. Targeting MSPs exponentially increased the reach and leverage of cyber extortionists—with the possibility of creating extreme tail risks that could become uninsurable without government support (Pal et al. 2021).

Countering 3rd-generation ransomware

The evolution of 3rd-generation ransomware coincides with the property and casualty insurance hard market and increased demand for cyber insurance (in part due to the increasing public attention to ransomware, thanks to the Colonial incident and many others). Several insurers have withdrawn from offering cyber insurance since its high point in 2018 (see Fig. 2). Insurers have also become more rigorous in their efforts to avoid shadow (or silent) cyber (e.g. Insurance Journal 2019) and formally exclude cover for state-sponsored activity (Lloyds Market Association 2021). The result is reduced insurance capacity in the property and casualty insurance market

at a time of increased demand for cyber insurance, leading to higher prices and the ability to impose strict underwriting conditions.

Although insurers have formally tightened underwriting conditions, in practice this is not at the expense of enterprise. For example, although leading cyber insurers now require customers to employ multifactor authentication as a condition of receiving insurance, underwriters reported to us that customers can easily comply by activating a feature in their existing software. Insurers also suspect that this requirement is unlikely to last once the hard market is over. Instead, the main developments have been sharply increasing the price charged for cyber insurance and strengthening the public–private partnership in fighting extortive cybercrime. The Ransomware Taskforce (2021)—a broad coalition of stakeholders from the public and private sectors including representatives from the insurance industry—stressed the need for governments to prioritise combatting ransomware and aggressively engaging with cybercriminals, as well as the states harbouring them. The Taskforce's 2021 report proposed that governments should encourage companies to prepare for and help them respond to ransomware attacks, as well regulate cryptocurrencies to disrupt the payments process.

The US government responded swiftly and aggressively to the heightened public concern about ransomware. In October 2021, a National Cryptocurrencies Enforcement Unit was created to investigate and prosecute criminal misuse of cryptocurrencies. In return, some insurance companies strengthened their incident response protocols to make the reimbursement of ransom payments conditional on notifying and cooperating with law enforcement. For example, the Lloyds Market Authority's 2021 "Guidance for Handling a Ransomware Incident" stresses the need to explore alternatives to paying ransoms, inform and share relevant information with the authorities, and avoid payments to sanctioned entities.

There have been some notable successes of the US authorities against ransomware groups. In January 2022, the Russian FSB searched 25 addresses, detained 40 suspects and charged two alleged members of the REvil Ransomware Group based on intelligence by the US. Even though there is no expectation that suspects would be extradited to the US, they could face up to seven years in prison in Russia. This has greatly reduced the expected profits from targeting larger organisations that could trigger political ire or law enforcement interest. Indeed, industry insiders saw a decided shift from "big game hunting" to "mid-game hunting" in the US in the second half of 2021 (Coveware 2021). As one Revil Associate put it in an interview published on Flashpoint (2021):

> … they don't want to draw attention to themselves. You can hit the jackpot once, but provoke such a geopolitical conflict that you will be quickly found. It is better to quietly receive stable small sums from mid-sized companies…

Although the total number of attacks remains high, reducing the incentives for ransomware threat actors to cause extreme damage may well prove sufficient to maintain the insurability of ransomware.

Ransomware, insurance and enterprise

Cyber insurance facilitates enterprise by providing money and expertise when a loss occurs and, sometimes, by providing loss prevention advice in advance. An insurer's loss prevention advice *should* be particularly valuable because it is "bonded", meaning that insurers in effect guarantee the advice by paying for the losses that result (Baker and Griffith 2010). Nevertheless, recent research reveals, and our discussions with insurers and vendors confirm, that policyholders tend not to take advantage of cyber insurers' loss prevention services, except in the context of recovering from a breach (Cunningham and Talesh 2021).

When we understand insurance as facilitating enterprise, this situation makes sense. Insurance buyers and sellers care about their enterprises, not loss prevention per se. When there's a breach, insurers' clients want all the help they can get in the context of their urgent need to get their business back online. Before a breach, insurers can only require loss prevention efforts that pay off in the form of premiums that are lower than the cost of the loss prevention. Otherwise, rational, reasonably informed buyers will go to insurers that don't require that loss prevention (insurance brokers know who those insurers are). Without meaningful premium reductions, buyers will undertake only those loss prevention efforts that make sense to them considering all the other pressing demands on their enterprise. An insurance buyer who wants to make investments in loss prevention might well consider advice from a cyber insurer, but if the advice isn't backed up by meaningful premium reductions or underwriting restrictions, the perceived value is diluted, no matter what insurance theorists might have to say about the bonded nature of that advice (Abraham and Schwarcz 2023).

An insurer who understands that customers ignore or downplay loss prevention advice will invest less time and effort in making and "selling" that advice, except to the extent that offering the advice helps market the insurance. That insurer will invest, however, in the services that customers need to keep their enterprises going: payment of the losses that do occur and access to (and payment for) services that help customers recover from those losses. In the ransomware context, breach response services provide high perceived value at low and, over the short time horizon of a cyber insurance policy, predictable cost, allowing insurers to provide meaningful value to customers while offering policy limits that are low compared to the limits in traditional property and liability policies offered to the same customers.

A mismatch between customers' potential losses and the limits of the cyber insurance on offer disrupts that equilibrium. That mismatch has already occurred with malware that insurers contend is state sponsored, such as Merck's alleged billion-dollar loss from NotPetya, and insurers' subsequent drafting of exclusions for state-sponsored losses. This mismatch is threatening to occur with other ransomware gangs and may shift the competitive equilibrium in the insurance market. Insurers no longer suffer competitive disadvantage from tightening their terms as they join forces to encourage the government to cut off the right tail of their ransomware losses (Government Accountability Office 2022).

An unanswered question is whether insurers will start working on ways to moderate ransom demands similar to the long-standing disruptive bargaining strategy in the K&R insurance market. K&R insurers used to provide insurance against cyber extortion. Their crisis responders naturally applied their ransom discipline ethos and bartered down hackers' demands—albeit at the price of longer business disruption and greater risk of triggering privacy breach lawsuits. Their approach—focused on reducing third-party moral hazard by lowering the returns from crime—lost out in the marketplace to the liability-focused cyber insurance. Can that K&R "DNA" be inserted back into cyber insurance?

Evolution through marketplaces differs from biological evolution—it is possible to recover and reinsert a feature that was selected out. But reinserting the K&R ransom DNA into cyber insurance may need some government action because of the outsized privacy risks illustrated by the effectiveness of the 3rd-generation ransomware's double extortion strategy. Otherwise, customers' enterprise needs will encourage shortcuts through or evasion of K&R's slower, more deliberate approach. Requiring disclosure to the government of ransomware demands and payments is a good first step (e.g. Schwarcz et al. 2023). That requirement would be even more effective if it could be coupled with a safe harbour from liability for businesses that cooperate with law enforcement, akin to the brownfield redevelopment safe harbours that we observed in our earlier research on the relationship between government and insurance (Baker and Shortland 2022). Such safe harbours cannot protect businesses from reputational harm or angry customers, but a broad-based ethic and practice of disclosure could reduce the reputational harm as customers and the public come to understand that even careful businesses can be victimised.

Conclusion

Insurance for ransomware nicely illustrates the evolutionary dynamic of insurance markets. Insurers shape the risk environment in which they operate, and they respond to changes other actors make in that environment. In the process insurers balance enterprise and security to maintain sustainable insurance markets. Recognising these dynamics deepens what it means to understand insurance-as-governance and what to expect from that governance. The primary function of commercial insurance has always been to promote enterprise, defined for present purposes as the objectives of the insured organisations. The insurance-as-governance literature has never suggested otherwise, even when that literature has employed a rational choice framework that focuses on insurers' role in loss prevention (e.g. Heimer 1985). Highlighting the centrality of enterprise to insurance may help prevent others from drawing the wrong conclusions.

In the process of promoting enterprise, insurers also promote security, primarily by providing customers with greater confidence in the sustainability of their enterprises. Insurers also engage in the loss prevention and mitigation activities that fit the narrower, more active meaning of the word "security" implicit in terms like data and computer security, but they engage in those security-oriented activities in the service of enterprise, including their own. If insurers do not see a payoff for their

own enterprise, they do not, and cannot be expected to, make the effort. For example, insurers' attention enterprise explains the abandonment of detailed risk assessments early in the development of the cyber insurance market, the decision to focus on loss mitigation rather than loss prevention, and the decision (so far) not to adopt the K&R insurers' approach to negotiation when resolving ransomware attacks.

In that regard, the insurance for ransomware experience that we report here provides support for one part of what Abraham and Schwarcz (2023) apparently intend as a critique of the insurance-as-governance research: why it is often not in insurers' interests to engage in the kinds of loss prevention efforts that security experts recommend and that governments more frequently mandate or undertake themselves. We find that cyber insurers only selectively engage in security efforts. Yet, their focus on creating protocols for cost reduction was dictated by the (artificially) high liabilities attached to publicising privacy breaches relative to the cost of paying ransoms (Baker and Shortland 2022). If this imbalance was addressed, for example by providing safe havens for companies choosing not to pay ransoms, it would create incentives to create governance infrastructures that help reduce the profitability of ransomware. For this, insurers might draw on the wealth of experience of Lloyd's insurers dealing with threat extortion.

We also find that, when ransomware threatened to become uninsurable, cyber insurers joined with computer security professionals to pressure governments to take action. This, too, can be understood as an example of insurance-as-governance: one that recognises the limits of private governance and overcomes a collective action problem by engaging and supporting the state.

Appendix 1: List of interviews

Insurance

1 Analyst, actuary and cyber services vendor.
2 Cyber risk specialist with US property insurer.
3 Cyber insurance underwriter with major US property insurer.
4 Head of cyber underwriting for North America.
5 Underwriter—cyber product line manager with 20 years of experience in cyber.
6 Cyber product manager with reinsurance company.
7 Head of cyber reinsurance at major broker.
8 Underwriting Manager, Facultative and Corporate Cyber.
9 Former Lloyd's special risks underwriter, current CEO of MGA for special risks.
10 Chief claims officer at cyber insurance company.
11 Former cyber underwriter and currently wholesale broker.
12 Former cyber underwriter and former CEO of MGA.
13 Veteran cyber broker.
14 Senior cyber underwriter for multiple insurers.
15 Enterprise Lead for Cyber Insurance.

Legal

16 Vice President, Litigation Manager and General Counsel.
17 Lawyer, breach response expert.

Security

18 Founder/CEO of breach responder.
19 Founder/CEO of Malicious risk consultancy.
20 Cybersecurity specialist and advocate.
21 CEO of network security services company.
22 Head of Cyber Response.
23 Project leader for Financial Crime and Security at thinktank.

Policy

24 Project leader for Cyber insurance at thinktank.
25 Global Head of Cyber Security for breach response company.

Appendix 2: List of workshops/conferences/events

(1) PLUS cyber symposium February 2019.
(2) Cyber insurance workshop at Penn Law School December 2019.
(3) "Ransomware: The Role of Cyber Insurance" Royal United Services Institute workshop (online) 17 February 2022.
(4) Ransomware Taskforce. Insurance subgroup (online) 16 March 2021.

Data availability In addition to the public sources cited in the text, this article draws on the confidential interviews and the workshopand conference listed in the appendix. Because of the confidential nature of the interviews and the ChathamHouse rules of the workshop conference, the notes from those interviews and events cannot be made available.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

Abraham, Kenneth S., and Daniel Schwarcz. 2021. Courting disaster: The underappreciated risk of cyber-insurance catastrophe. *Connecticut Insurance Law Journal* 27 (1): 51.

Abraham, Kenneth, and Daniel Schwarcz. 2023. The limits of regulation by insurance. *Indiana Law Review 98*. https://ssrn.com/abstract=4119812.

Arrow, Kenneth. 1963. Uncertainty and the welfare economics of medical care. *American Economic Review* 53: 943–971.

Avraham, Ronen, and Ariel Porat. 2022. *The dark side of insurance*. Working paper.

Baker, Tom. 2019. Back to the future of cyber insurance. *PLUS Journal*, Q3. https://scholarship.law.upenn.edu/faculty_scholarship/2184.

Baker, Tom. 2021. Uncertainty > risk: Lessons for legal thought from the insurance runoff market. *62 Boston College Law Review* 62: 59.

Baker, Tom, and Sean Griffith. 2010. *Ensuring corporate misconduct: How liability insurance undermines shareholder litigation*. Chicago: University of Chicago Press.

Baker, Tom, and Kyle Logue. 2017. *Insurance law and policy: Cases, materials and problems*, 4th ed. Boston: Aspen Publishing.

Baker, Tom, and Anja Shortland. 2022. Dimensions of government support in insurance as governance regimes: Lessons for ransomware. *Regulation and Governance* (accepted).

Beamon, Craig, Ashley Barkworth, Toluwalope David Akande, Saqib Hakak, and Muhammad Khurram Khan. 2021. Ransomware: Recent advances, analysis, challenges and future research directions. *Computers and Security* 111: 102490.

Ben Shahar, Omri, and Kyle Logue. 2012. Outsourcing regulation: How insurance reduces moral hazard. *University of Michigan Law Review* 111: 197–248.

Betterley, Richard. 2001–2021. *The Betterley Reports: Cyber risk market survey*.

Coveware. 2018a. We hear this story. OFTEN. *Coveware Blog*, 7 May. https://www.coveware.com/blog/2018a/5/8/we-hear-this-story-often-wp4ne. Accessed 11 Oct 2022.

Coveware. 2018b. Beware of dishonest ransomware recovery firms. *Coveware Blog*, 11 Dec. https://www.coveware.com/blog/2018b/12/11/beware-of-dishonest-ransomware-recovery-firms. Accessed 11 Oct 2022.

Coveware. 2019. *GandCrab v5.1 exploit kit distribution and TOR site features*. Coveware Blog, 5 Feb. https://www.coveware.com/blog/2019/2/4/gandcrab-51. Accessed 11 Oct 2022.

Coveware. 2021. Ransomware attackers down shift to 'Mid-Game' hunting in Q3 2021. *Coveware Blog*, 21 Oct. https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts. Accessed 11 Oct 2022.

Coveware. 2022a. Ransomware as a service innovation curve. *Coveware Blog*, 27 Jan. https://www.coveware.com/blog/2022a/1/26/ransomware-as-a-service-innovation-curve. Accessed 11 Oct 2022a.

Coveware. 2022b. Law enforcement pressure forces ransomware groups to refine tactics in Q4 2021. *Coveware Blog*, 3 Feb. https://www.coveware.com/blog/2022b/2/2/law-enforcement-pressure-forces-ransomware-groups-to-refine-tactics-in-q4-2021. Accessed 11 Oct 2022b.

Cunningham, H. Bryan., and Shauhin A. Talesh. 2021. Uncle Sam RE: Improving cyber hygiene and increasing confidence in the cyber insurance ecosystem via government backstopping. *University of Connecticut Insurance Law Journal* 28: 1–84.

Daston, L. 1987. The domestication of risk: Mathematical probability and insurance. In *The probabilistic revolution*, ed. Lorenz Krüger, 237–260. Cambridge: MIT Press.

Dudley, Renee. 2019. *The extortion economy: How insurance companies are fueling a rise in ransomware attacks*. New York: ProPublica.

Ericson, Richard, and Aaron Doyle. 2004. *Insurance as governance*. Toronto: University of Toronto Press.

Ewald, Francois. 2020/1986. *The birth of solidarity: The history of the French welfare state*. Durham: Duke University Press.

Ewald, Francois. 1991. Insurance and risk. In *The Foucault effect: Studies in governmentality*, ed. Graham Burchell, Colin Gordon, and Peter Miller. Ann Arbor: University of Michigan.

Filiz, Burak, Budi Arief, Orcun Cetin, and Julio Hernandez-Castro. 2021. On the effectiveness of ransomware decryption tools. *Computers and Security* 111: 102469.

Flashpoint. 2021. Russian hacker Q&A. *Blog*, 29 Sep. https://www.flashpoint-intel.com/blog/interview-with-revil-affiliated-ransomware-contractor/. Accessed 11 Oct 2022.

Froomkin, Michael A. 1995. The metaphor is the key: Cryptography, the clipper chip and the constitution. *University of Pennsylvania Law Review* 143: 709.

Fuentes, Mayra, Feike Hacquebord, Stephen Hilt, Ian Kenefick, Vladimir Kropotov, Robert McArdle, Fernando Mercês, and David Sancho. 2021. Modern ransomware's double extortion tactics and how to protect enterprises against them. *Trend Micro Research.* https://documents.trendmicro.com/assets/white_papers/wp-modern-ransomwares-double-extortion-tactics.pdf. Accessed 17 Oct 2022.

Government Accountability Office. 2022. *Cyber insurance: Action needed to assess potential federal response to catastrophic attacks*. GAO-22-104256.

Guidewire. 2020. Taming the uncertainty of ransomware risk. White paper. *Guidewire.* https://www.guidewire.com/blog/industry-trends/taming-uncertainty-ransomware-risk-part-1/. Accessed 17 Oct 2022.

Hampton, Nikolai, and Zubair A. Baig. 2015. Ransomware: Emergence of the cyber-extortion menace. In *Paper presented at the 13th Australian information security management conference*, Edith Cowan University Joondalup Campus, Perth, Western Australia, November 30–December 2.

Heimer, Carol. 1985. *Reactive risk and rational action: Managing moral hazard in insurance contracts*. Chicago: University of Chicago Press.

Holdsworth, William Searle. 1917. The early history of the contract of insurance. *Columbia Law Review* 17 (2): 85–113.

Insurance Journal. 2019. Two new London Market model cyber exclusion clauses published by IUA. *Insurance Journal*, June 6.

Karten, Walter T. 1997. How to expand the limits of insurability. *The Geneva Papers on Risk and Insurance: Issues and Practice* 85: 515–522.

Kharraz, Amin, William Robertson, Davide Balzorotti, Leyla Bilge, and Engin Kirda. 2015. Cutting the Gordian knot: A look under the hook of ransomware attacks. In *Proceeding of the 12th conference on detection of intrusion and malware, and vulnerability assessment 2015 s*, ed. Magnus Almgren, et al., 3–24. New York: Springer.

Knight, Frank. 1921. *Risk, uncertainty, and profit*. Eastford: Martino Fine Books.

Krebs, Brian. 2010. I'll take two mastercards and a visa please. *Krebs on Security Blog*, 22 Sep. https://krebsonsecurity.com/2010/09/ill-take-2-mastercards-and-a-visa-please/. Accessed 10 Oct 2022.

Krebs, Brian 2022. Conti ransomware group diaries, Part III: Weaponry. *Krebs on Security Blog*, 22 Sep. https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry/. Accessed 11 Oct 2022.

Lloyd's Market Association. 2021. *Cyber war and cyber operation exclusion clauses*. Lloyd's Bulletin, 25 November 2021 LMA21-042-PD.

Lusthaus, Jonathan. 2018. *Industry of anonymity: Inside the business of cybercrime*. Cambridge: Harvard University Press.

Majuca, Ruporto, William Yurcik, and Jay P. Kesan. 2006. The evolution of cyberinsurance. *Cornell.edu*, 6 Jan.

O'Malley, Pat. 1991. Legal networks and domestic security. *Studies in Law, Policy and Society* 11: 171–190.

Pal, Ranjan, Ziyuan Huang, Sergey Lototsky, Xinlong Yin, Mingyan Liu, Jon Crowcroft, Nishanth Sastry, Swades De, and Bodhibrata Nag. 2021. Will catastrophic cyber-risk aggregation thrive in the IoT age? A cautionary economics tale for (re-)insurers and likes. *ACM Transactions on Management Information Systems* 12 (2): 1–36.

Paquet-Clouston, Masarah, Behard Hslhofer, and Benoit Dupont. 2018. Ransomware payments in the Bitcoin ecosystem. In *Paper presented at the 17th annual workshop on the economics of information security*, June 2018.

Parchomovsky, Gideon, and Peter Siegelman. 2022. Third party moral hazard. *The Journal of Legal Studies* (forthcoming).

Popper, Nathaniel. 2015. *Digital gold: Bitcoin and the inside story of the misfits and millionaires trying to reinvent money*. New York: Harper Paperbacks.

Reuters. 13 May 2021. Colonial Pipeline has cyber insurance policy—Sources. https://www.reuters.com/business/energy/colonial-pipeline-has-cyber-insurance-policy-sources-2021-05-13/. Accessed 10 Oct 2022.

Richardson, Ronny, and Max M. North. 2017. Ransomware: Evolution, mitigation and prevention. *International Management Review* 13: 10–21.

Rossi, Michael. 2000. *Bringing order to chaos: Insurance issues for e-commerce activities*. IRMI. https://www.irmi.com/articles/expert-commentary/insurance-issues-for-e-commerce-activities. Accessed 10 Oct 2022.

Rossi, Michael. 2001. *New stand-alone e-commerce insurance policies for first-party risks*. IRMI. https://www.irmi.com/articles/expert-commentary/new-stand-alone-e-commerce-insurance-for-first-party-risks. Accessed 10 Oct 2022.
Romanosky, Sasha, Lillian Ablon, Andreas Kuehn, and Therese Jones. 2019. Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity* 2019: 1–19.
Schwarcz, Daniel, Josephine Wolff, and Daniel Woods. 2023. How privilege undermines cybersecurity. *Harvard Journal of Law and Technology*. https://doi.org/10.2139/ssrn.4175523.
Shavell, Steven. 1982. On liability and insurance. *The Bell Journal of Economics* 13 (1): 120.
Shortland A. 2017. Governing kidnap for ransom: Lloyd's as a "private regime" *Governance* 30(2): 283–299.
Shortland, Anja. 2019. *Kidnap: Inside the ransom business*. Oxford: Oxford University Press.
Shortland, Anja. 2021. *Lost art: The art loss register's case book*, vol. 1. London: Unicorn.
Simon, Jonathan. 1994. In place of the parent: Risk management and the governance of campus life. *Social and Legal Studies* 3: 14–45.
Voreacos, David, Katherine Chiglinsky, and Riley Griffin. 2019. Merck cyberattack's $1.3 billion question: Was it an act of war? *Bloomberg*, December.
Waddell, Kaveh. 2016. The computer virus that haunted early AIDS researchers. *The Atlantic*, 10 May.
Watkins, Ali, and Benjamin Weiser. 2022. Inside the Bitcoin laundering case that confounded the Internet. *The New York Times*, February.
Wilding, Edward. 1990. Trojan Horse: AIDS disk. *Virus Bulletin* January 1990: 3–7.
Wolff, Josephine. 2022. *Cyber-insurance policy: Rethinking international risk for the Internet age*. Cambridge: MIT Press.
Woods, Daniel, and Rainer Böhme. 2021. How cyber insurance shapes incident response: A mixed methods study. In *Workshop on the economics of information security (WEIS)*, 2021.
Yost, Paula, Paul E.B.. Glad, and William T. Barker. 2001. In search of coverage in cyberspace: Why the commercial general liability insurance policy fails to insure lost or corrupted computer data. *SMU Law Review* 54: 2055–2085.
Young, Adam, and Moti Yung. 1996. Cryptovirology: Extortion-based security threats and countermeasures. In *Proceedings of the IEEE symposium on security and privacy*, 1996, #129140.
Young, Adam, and Moti Yung. 2017. Cryptovirology: The birth, neglect, and explosion of ransomware. *Communications of the ACM* 60 (7): 24–26.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

About the authors

Tom Baker is the William Maul Measey Professor at the University of Pennsylvania Carey Law School. He studied sociology and law at Harvard, where he received his BA and JD. Tom's research explores insurance law, institutions and markets using methods from history, economics, psychology and sociology. One of the first scholars to study insurance-as-governance, Tom's prior work addresses many topics in the insurance field, including the impact of insurance on civil litigation, the historical development of insurance institutions and ideas, the behavioural economics of insurance and insurance company restructuring.

Anja Shortland is a Professor in Political Economy at King's College London. She studied Engineering Science at Oxford and for her MSc in Political Economy and PhD in International Relations at LSE. Anja specialises in institutional economics and the economics of crime. She is fascinated by private ordering in the world's trickiest markets: hostages, hijacked ships, stolen art, looted antiquities and ransomware. Her research focuses on trades between legal and illegal enterprises and insurance-as-governance in criminal markets.