A History of Cyber Risk Transfer

DANIEL W. WOODS, University of Edinburgh, UK and British University in Dubai, UAE
JOSEPHINE WOLFF, Tufts University, USA

Cyber risk management involves balancing risk acceptance, avoidance, reduction and transfer. Academic researchers have focused on risk reduction measures. Studies of cyber risk transfer are less common, mainly centering on cyber insurance. This emphasis on risk reduction overlooks the development of many real-world cyber risk transfer products in the last decade. Our study describes the emergence of products including: warranties, cloud computing partnerships, parametric insurance, reinsurance, and cyber cat bonds. We characterize how these solutions addressed four core challenges of transferring cyber risk: (1) tailoring coverage to the threat landscape; (2) managing solvency; (3) data collection for risk assessment; and (4) creating incentives for risk reduction. The result is an integrated history of cyber risk transfer describing how novel products and partnerships emerged to address failings in prevailing business models. Our descriptive study can help other researchers to understand real-world problems, providing a foundation for future research and a richer picture of the overall cyber risk transfer landscape, as well as a deeper understanding of the types of cyber risk that can—and cannot—be effectively transferred.

1 INTRODUCTION

The idea that "information security is risk management" was presented as a new security paradigm in 2001 [1]. This involved acknowledging that security risk in real-world systems cannot be eliminated and must instead be managed. The approach gained momentum over time [2, 3] and has become the mainstream approach to cybersecurity [4, 5]. Risk management theory raises four broad options for treating cyber risks: accept, reduce, transfer or avoid.

The vast majority of cyber risk research focuses on risk reduction solutions, under the banner of computer, information and/or cyber security. Entire conferences and workshops are dedicated to sub-areas of cybersecurity including "operating system security, access control, network security, intrusion detection" [6]. Research into cyber risk transfer is comparably rare and has revolved around a single type of insurance, namely indemnity products.

Since the 1990s, standalone cyber insurance has evolved to address emerging cybercrimes like data breaches and ransomware. Over the course of that evolution, novel cyber risk transfer vehicles have emerged to support and challenge indemnity insurance. Figure 1 displays a timeline showing that the first cyber warranty, parametric product, and cat bond were announced in 2014, 2019, and 2023 respectively.

Our study characterizes how and why these different cyber risk transfer products emerged, evolved, and, in some cases, failed. This is structured around four challenges, namely coverage, solvency, data collection, and incentives. We provide an integrated account of how early cyber risk transfer vehicles succeeded and failed at solving each challenge, which in turn created business opportunities for novel solutions.

Section 2 describes our analytical approach. Section 3 sketches how cyber insurance has evolved through three separate phases that centered on: experimentation, data breaches, and ransomware. Section 4 describes how cybersecurity firms responded by announcing warranties. Section 5 examines the niche market for parametric cyber insurance. Section 6 looks at how insurers transferred cyber risk to reinsurers. Section 7 identifies mechanisms to transfer cyber risk to investors. Finally, Section 8 distils some central cyber risk-related themes, lessons, and research goals from the different risk transfer products.

Reference: Woods, D.W. and Wolff, J., 2024, April. A History of Cyber Risk Transfer. In *Workshop on the Economics of Information Security (WEIS2024).*

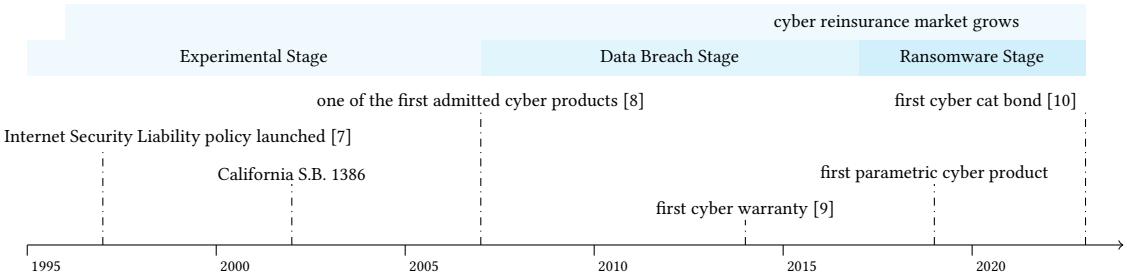

Fig. 1. Key events and stages in the history of cyber risk transfer. All claims to *first* are based on the reference and may be contested.

2 APPROACH

Section 2.1 describes how we collected the information that informs the historical narrative. This was structured according to a conceptual framework derived from the economics of security [11, 12], which we describe in Section 2.2. We also explain key terms in Table 1.

2.1 Analysis

This project was guided by background research carried out over the last eight years by the authors. This involved various qualitative and quantitative research studies in the area of cyber risk transfer. Conducting and sharing this research provided a working understanding of how these products emerged.

The first step in this research project involved identifying the products of interest: indemnity insurance, warranties, partnerships with cloud vendors, parametric insurance, reinsurance, and capital market products. After further research, we decided to integrate cloud partnerships into the indemnity insurance section as these partnerships transfer risk to an insurer not the cloud company.

The second step involved describing the history and characteristics of each product. Our main information sources were academic publications and public statements made in press releases and media reporting, typically related to new product announcements. Public sources provide an opportunity for other market participants to respond, unlike, for example, a single-stage research study relying on anonymized interviews conducted in private. This allowed us to capture different perspectives on the same topic, such as the public discussion about the value of cyber warranties among InfoSec vendors and insurers in Section 4 [13, 14]. We decided to attribute statements to individuals and companies in line with the original source. Despite our efforts, the sources are neither comprehensive or authoritative. We expect that other authors will write different histories, a possibility we discuss in Section 8.

Based on these sources, we tried to build a timeline by identifying the 'first' product for each section.[1] Due to the relative age and market size, cyber insurance developed more than the others and so we divided this history into three stages. We then tried to characterize how the product functioned, typically focusing on the supplier rather than the buyer. To facilitate comparison across products, we structured the historical narrative according to a defined framework, which we now describe.

[1]This is another topic that will no doubt generate debate, which we welcome.

Terminology	Intuition
Primary Risk Transfer	These policies are bought by businesses to manage operational risk.
Indemnity Insurance (Section 3)	A policy in which the insured's payment is determined by the size of the loss suffered by the insured.
Warranty (Section 4)	A guarantee that the customer will be compensated for a failure in the vendor's product or service.
Parametric Insurance (Section 5)	A policy in which a fixed payment is triggered by a pre-defined event, independent of the insured's loss.
Higher Layer Risk Transfer	These instruments are bought/issued by (re)insurers to manage insurance portfolio risk.
Reinsurance (Section 6)	A policy bought by an insurer to cover insurance losses.
Retrocession	A policy bought by a reinsurer to cover reinsurance losses.
Quota Share Reinsurance	A policy in which the insurer and reinsurer share premiums and losses in a fixed proportion.
Excess of Loss (XoL) Reinsurance	A policy in which the insurer is compensated when portfolio losses exceed a specified limit.
Capital Markets (Section 7)	An umbrella term for (re)insurers transferring portfolio risk to public and private investors.
Cat Bond	A fixed-income product structured so the buyer receives a lower return if a defined catastrophe occurs.
Portfolio Reporting	Statistics summarizing the performance of an insurance portfolio.
Gross Written Premium	Total premiums that customers will pay from policies issued in a time period (a year in Table 2).
Loss Ratio	Total claims costs (indemnity payments plus administration) divided by total premiums in a time period.

Table 1. Explanation of the intuition behind risk transfer terminology. Refer to other sources for technical definitions [24, 25].

2.2 Framework

Cyber risk transfer products can be evaluated in terms of how they address four core challenges: (i) coverage; (ii) solvency; (iii) data collection; and, (iv) incentives. These categories are derived from literature on the economics of information security [12]. We do not claim these categories are exhaustive or even disjoint.[2]

The first challenge is to craft *coverage* that addresses the threat landscape and satisfies the demands of risk holders. Gaps in coverage from traditional products emerged as insurers fought legal cases to exclude losses caused by data breaches and other cyber perils [7]. The coverage of cyber risk transfer vehicles must evolve over time as threat actors pivot to new cyber crimes [15, 16].

The second challenge, *solvency*, is to balance satisfying customer demand against paying out to customers. Risk transfer providers must price risk to make a profit in typical years and also make sure funds are available if catastrophe strikes. The potential for cyber catastrophe results from shared technologies and service providers [17, 18]. This can be addressed by providers either holding capital buffers or by using a risk transfer vehicle, such as buying reinsurance or issuing a cat bond.

To solve *data collection*, risk transfer providers must create infrastructure to assess both the threat landscape and the digital infrastructure of customers. This involves measuring the frequency and impact of covered risk, as well as the efficacy and implementation of risk controls. This is challenging because of a lack of reliable data about cyber risk [19], in part because firms are unwilling to share information [20]. Scientific studies of cyber risk are also under-developed [21].

Solving the fourth challenge involves risk transfer providers actively creating *incentives* to improve security and avoid losses. This has theoretical roots in mechanism design, whereby economists try to create an incentive regime that ensures a particular outcome. It has long been predicted that insurers would do so [22, 23], such as by offering premium discounts if firms improve security.

[2]Creating an incentive regime often requires some level of data collection to ensure enforcement. Similarly, marketing is a business function that sits outside our framework.

3 CONVENTIONAL INSURANCE

To capture the evolution of conventional cyber insurance since the late 1990s[3], we introduce a stylized three-stage model of development to capture broad trends, acknowledging that exceptions likely exist.

3.1 Experimental Cyber (1997-2006)

In the early years, there was no unified view of which risks cyber policies should cover. Baker observes that "the mature [insurance] product may not look much like the lightbulb that went off in the heads of the underwriters who invented it", which was borne out by cyber insurance [26].

Coverage Initially, three of the biggest companies in the insurance industry had differing views on what would become the main cyber claims drivers. Leib Dodell, a corporate leader at Chubb, imagined cyber insurance would cover media liability resulting from firms publishing on the Internet [26]. An alternative vision was provided by Ty Sagalow at AIG, who "wanted to cover the business interruption loss of a distributed denial of service attack" [27]. In contrast, Emily Freeman and her colleagues at Marsh created a product covering "downtime from hacking, fraud, and viruses, with some liability and privacy loss protection" [26]. These differing views on what cyber insurance should cover during the early days of the market illustrates the first challenge insurers faced, namely crafting coverage for an emerging and rapidly shifting threat landscape. Even though the visions of leaders from Chubb and AIG did not come to pass, these firms went on to become the first and fifth largest US-domiciled cyber insurance providers (see Table 2).

Solvency In the late 1990s and early 2000s, insurers wrote few policies with low coverage limits relative to other corporate lines. Large multi-line insurers were comfortable writing a relatively small cyber portfolio with limited outstanding limit, not least because the product was highly profitable. For example, AIG reportedly achieved "$100 million in sales at 11% loss ratio" [27] around the turn of the century. Anecdotal evidence suggests these insurers also bought primitive reinsurance policies (see Section 6 for more details).

Data Availability During this experimental stage, actuarial modeling based on a lack of data was tolerated. In part, this was because insurers viewed selling cyber insurance as a way to build a claims data set. It is worth quoting Sagalow on pricing initial cyber insurance at length:

> "we had to make certain assumptions and we made certain analogies. So first on severity, we assumed that a client would be able to prove the amount of loss income in the same way they would if there was a fire. So we had to then decide, well, how long would this fire last? And then we had to decide how often it was. And we talked to a number of CTOs and CIOs and just made an assumption on how a denial of service attack would compare to having a fire, both in terms of length of recovery time as well as frequency. And of course it was a complete guess..." [27]

In addition, many insurers used audits to collect information about security practices. For instance, the insurance carrier Hiscox assessed the security of its own policyholders and also the security of their Internet service providers before deciding whether to issue a policy [7, p.44].

Incentives These audits and assessments often created financial incentives to improve security. For example, AIG offered a 25% discount to customers whose security was audited and certified by the National Computer Security Association [7, p.28]. Broker InsureTrust would have its own auditors perform a series of tests on clients' networks and then instruct those clients on how to "rebuild" their computer networks to be more secure. These auditing efforts

[3]Cyber coverage was available under composite policies before this. For example, so-called Bankers Blanket Bond (BBB) policies covered banks for fraud and dishonesty losses including Computer Fraud, with Lloyd's of London standardizing an endorsement in 1998.

were often rigorous, time-intensive, and expensive, with one insurer estimating in 2000 that "the best-performing insurance companies spend up to 30 cents of each premium dollar helping clients reduce loss probability" [7, p.45]. These high-touch consulting services would give way to automated services as insurers started to sell to smaller firms.

3.2 Data Breach Insurance (2007-2017)

An intuitive end to the experimental phase is when regulators first accepted cyber insurance policies as admitted products in the US.[4] Once approved, admitted products limit the freedom of insurers to experiment by adjusting policy language and pricing. We are not aware of anyone claiming to have identified the very first admitted cyber policy, but a good enough answer is provided by Romanosky et al. [8]. Their study systematically collected admitted insurance policies from the three largest US states, identifying the first policy in 2007.

Coverage Romanosky et al. [8] also analyzed the coverage found in each policy. They found "somewhat consistent" coverage across cyber insurance products that typically covered third-party costs like "[regulatory] penalties, [litigation] defense and settlement costs", as well as breach notification costs [8]. First-party coverage for costs like business interruption, data/system restoration and ransom extortion payments were available in some but not all policies [8].

In addition to being the year of the first admitted policy, 2007 is also the time when more than half of the states in the US had passed data breach notification laws [28]. Famous examples of data breaches included the theft of 45.6 million payment card numbers from retail chain TJX Companies Inc. in 2006, the theft of more than 100 million payment card numbers from Heartland Payment Systems in 2008, and the loss of personal records about 76 million veterans by the National Archives and Records Administration in 2009, among others [29]. Since the primary motive for these breaches was financial [30], and large organizations typically stored more payment card records than small ones, large organizations were much more likely to be victimized [31]. Large firms were also more likely to purchase insurance, in part due to increased concerns about class action lawsuits.

Solvency These large firms demanded higher coverage limits ($50 million plus), which created problems for individual insurers who wanted to diversify the risk across customers. This was solved, in part, by so-called *tower policies* in which different insurers wrote different slices of coverage, according to their risk appetite. For example, the primary (lead) insurer might write the first $10 million of losses after the deductible. Another insurer would take the losses between $15 and $25 million, a third insurer would cover the next $25 million and so on.

Even so, some policyholders were unable to purchase as much coverage as they wanted. For instance, at the time of its data breach in 2013, Target had only managed to "cobble together" $100 million in cyber insurance coverage from multiple carriers, and had been turned away by other carriers when it tried to purchase even more [32]. Following the Target breach, many insurers scaled back the coverage they were willing to make available through towers. In 2014, it was reported that where businesses might once have been able to obtain between $300 and $350 million in cyber insurance, they were now often only able to secure a tower of around $250 million, maximum [33]. To manage this exposure, insurers relied on quota-share reinsurance, which comprised 95% of the reinsurance market in 2017 [34] (see Section 6 for more details).

Data Collection Despite the growing number of data breaches being publicly reported, insurers still used surprisingly unreliable data sources. The data sources for actuarial models that were reported to regulators included:

[4]This meant the product's policy wording and pricing was licensed by the insurance commissioners of the states in which the carriers operate. Although, the process varies across states.

Insurer	Gross Written Premium ($m)					US Market Share (%)					Loss Ratio (%)				
	2018	2019	2020	2021	2022	2018	2019	2020	2021	2022	2018	2019	2020	2021	2022
Chubb	321	355	404	473	605	16.0	15.8	14.7	9.8	8.6	28.6	27.7	61	76.9	53.8
Fairfax Financial	38	65	109	436	563	1.9	2.9	3.9	8.7	8.4	23.4	51.6	55.7	51.9	54.0
AXA	256	230	293	421	527	12.7	10.2	10.6	8.7	8.0	57.2	65.7	98.2	86.5	66.2
Tokio Marine	45	47	78	250	368	2.2	2.1	2.8	5.2	5.1	30.5	17.1	51.1	43.8	57.8
Arch	-	-	-	172	346	-	-	-	3.2	4.8	-	-	-	9.2	52.3
Travelers	146	179	206	232	315	7.3	8.0	7.5	4.8	4.4	22.5	32.1	85.5	72.7	34.8
AIG	232	226	228	241	299	11.5	10.1	8.3	5	4.2	36.1	55.4	100.6	130.6	47.6
CNA	83	95	120	181	229	4.1	4.2	4.3	3.8	3.4	26.8	33.2	105.7	87.5	26.5
Liberty Mutual	66	69	42	138	208	3.3	3.1	2.3	2.9	2.9	63.2	38.9	23.3	30	95.2
Axis Capital	76.4	98	134	159	196	3.8	4.4	4.8	3.3	1.5	7.1	18.5	46.2	105.2	85.9
Beazley	111	151	177	201	175	5.5	6.7	6.5	4.2	2.9	7.8	22.0	47.9	38.7	19.6
Nationwide	-	-	-	-	257	-	-	-	-	3.7	-	-	-	-	12.5
Sompo	34	50	73	134	248	1.7	2.2	2.6	2.8	3.1	56.7	29.3	114.1	54.3	50.1
Zurich	43	44	64.4	-	152	2.1	2.0	2.3	3.1	-	18.2	86.9	40.4	76.9	-
Hartford Fire	40	50	103	123	152	2.0	2.2	3.7	2.6	2.2	16.4	31.6	25.4	16.3	15.5
BCS	70	76	87	132	-	3.5	3.4	3.1	2.7	10.4	-	33.0	59.1	80.1	-

Table 2. Data extracted from the US National Association of Insurance Commissioners' reports on the cyber insurance market.

> "(i) ... external sources [surveys and/or publicly reported breaches], (ii) estimated or guessed, (iii) looked to competitors, (iv) leveraged the experience of their own underwriters, and (v) adapted prices from other insurance lines." [8]

Many underwriters lacked historical data, with one insurer claiming "we have not experienced any claims over the past three years" [8]. But this lack of claims data did little to deter insurers from selling policies—quite the opposite, in fact; it suggested that insurers were unlikely to have to pay out many claims, fueling insurers' optimism about this new product. Entrepreneurial insurers accepted the uncertainty [26], in part because cyber insurance was proving to be profitable over time. In 2018, the median loss ratio for cyber insurance policies in the US was 35%, compared to 62% for property and casualty policies, according to a report by Aon [35]. Figure 2 shows cyber insurance pricing was relatively stable from 2014 to 2018, which is backed up by a study of prices filed with regulators [36].

Incentives This influx of insurers created a soft market (meaning lower prices and broader coverage) that reduced the ability of insurers to require policyholders to follow security procedures or even collect risk information from their policyholders [37, 38]. Rather than the hands-on audits and assessments that insurers had used in earlier years when they had fewer policyholders to assess, many carriers relied on questionnaires to assess the security postures of would-be policyholders. Firms purchased policies from the insurers who had the shortest questionnaires and required the fewest security controls, creating a race-to-the-bottom [37, 39].

Despite having little influence on pre-breach security levels, insurers did influence how policyholders responded to incidents. Most insurers provided access to a breach panel, a list of incident response (IR) firms whose fees the policy would cover [40]. Insurers used market power to negotiate lower prices, and also monitored the IR firms' service quality across multiple claims [41]. Some insurers found that during this period, early involvement of a lawyer was the most effective way to reduce the costs and risk of litigation following a data breach [40]. Many insurers set up their incident response mechanisms accordingly, with an emphasis on involving lawyers immediately rather than mandating

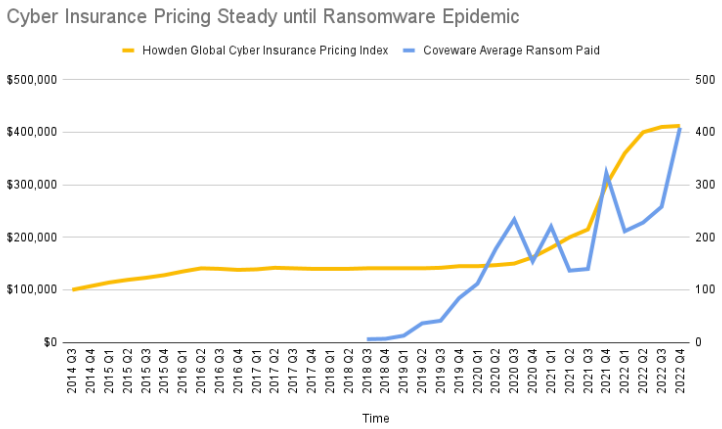

Fig. 2. Mean and median ransom payment according to Coveware, a ransomware negotiation firm.

pre-breach security controls [7]. This was a rational response to a threat landscape in which breach litigation was the main claims driver.

3.3 The Ransomware Epidemic (2018—)

From 2018 onward, the threat landscape shifted as ransomware became the biggest loss driver. Figure 2 shows how gangs succeeded in demanding ever greater ransoms. Ransomware gangs did not discriminate, which meant that smaller organizations also suffered first-party losses.

Some insurers responded by partnering with Managing General Agents (MGAs) who specialized in building technological solutions [42], essentially out-sourcing underwriting to an InsurTech firm. Other insurers acquired cyber MGAs [43]. A more recent trend has been insurers partnering with technology companies, both cybersecurity [44] and cloud vendors [45, 46], to get direct access to their customers' security data in order to offer carriers an even more detailed picture of their policyholders' security postures.

Coverage As previously mentioned, many policies already covered first-party losses [8]. The main shift was in what drove claims, which shifted to predominantly ransomware and fraudulent wire transfers caused by social engineering. As Baker observes [26], the expanded cyber insurance product was closer to Freeman's vision of a blended first- and third-party cyber insurance product covering downtime from incidents, as well as liability from any resulting litigation. This threat landscape impacted businesses of all sizes across every industry sector, unlike breach litigation that predominantly impacted large firms holding sensitive data [31]. The increased demand for policies that covered a growing number of risks faced by a wide variety of organizations caused the market to expand. Still, there were some costs that most insurers generally refused to cover—for instance, losses of intellectual property and trade secrets. But as part of a partnership with their cloud vendor, Google cloud customers could become eligible for an exclusive "specialized cyber insurance policy" called Cloud Protection +, which provided additional coverage, including compensation for trade secret loss [47]. An open question is how meaningful this additional coverage is in actuality.

Solvency The growth in the size of the market increased the risk of cyber catastrophe. Various realistic disaster scenarios were published [48], in which experts imagine a specific large scale cyber attack and try to model the

consequences. With time, natural catastrophe modeling firms developed stochastic models that allowed insurers and reinsurers to model how a catastrophic events could impact the policies they had underwritten. Insurers typically managed cat exposure by purchasing cyber reinsurance. For example, "over 75% of cyber insurers transfer[red] risk to reinsurers" by 2018 [49]. The importance of reinsurance is evidenced by SwissRe estimating that half of all cyber insurance premiums ultimately flowed to a reinsurer by 2020 [50].

There is a question about whether partnering with cloud service providers increases correlated losses related to a single outage or attack[5]. However, increased exposure to a single cloud provider could be beneficial if that provider is particularly responsible for improving customer's security posture [51]. For example, one InsurTech firm found that "organizations that used Google Workspace experienced the lowest frequency of incidents" [52]. Insurers limited the availability of these cloud partnerships.[6]

Data Collection The shift to insuring smaller firms and the rise of technology-focused MGAs aided actuarial modeling. The problem with insuring large firms is heterogeneity as these firms had the resources to develop custom IT infrastructure tailored to business needs and historic mergers. Further, the models were trained on a handful of data points because there are only so many US-based retailers with $100 billion or more in revenue. This combination of heterogeneity and small data sets limits actuarial science. In contrast, small firms tend to adopt commoditized IT solutions and there are more data points upon which to train models.

MGAs took advantage of these factors, and also the ability for automated data collection. Instead of asking for a questionnaire that had to be manually filled out, MGAs asked for the insured's email domain and collected data via Internet scans. It is notable that InsurTech firms do not typically complain about a lack of data.

When ransomware claims spiked for insurers in 2019 and 2020 (see Figure 2), the limitations of the data that insurers had collected came under closer scrutiny. Most carriers had failed to predict the surge in ransomware and reacted by significantly increasing their premiums but were not confident in their ability to model the rates of ransomware attacks. One insurer said, "When we got our shirts handed to us by ransomware in 2020, we overhauled our ransomware underwriting model and strategy . . . But candidly, it was from my understanding and not from real data" [54].

Cloud company partnerships could improve on prevailing data collection methods because the data provided by cloud providers is not self-reported and can be collected regularly, not just when policies are renewed like with questionnaires [55]. These partnerships also make it easier to enforce and verify whether policyholders implement certain required security behaviors, which mainstream insurers did not previously have the ability to do at scale.

Incentives Insurers use the available data sources to try to guide policyholders towards improved security practices. External network scans enabled one InsurTech to notify policyholders about "vulnerabilities and ports exploited by ransomware groups resulted in a 65% drop in ransomware-related claims from April to September 2020" [38]. There were also reports that purchasing cyber insurance could be conditioned on policyholders implementing "multi-factor authentication (MFA) as well as endpoint detection and response" [56]. Partnerships with IT vendors, such as the main email providers like Google and Microsoft, could allow insurers to directly measure configuration details like whether MFA is enabled, and thereby enable them to create incentives for better security by adjusting premium pricing according to policyholders' cloud configurations.

[5]Cloud providers run geographically distributed data centers and employ highly-resource security and reliability teams. To date, there has been no outage impacting all data centers at one provider. Therefore, it is erroneous to consider failures at individual data centers as perfectly correlated, and it can be argued this risk is largely uncorrelated.

[6]For instance, the Google Cloud partnership was initially available only to US customers with revenue between $500 million and $5 billion, and it only offered up to $50 million primary capacity [53].

3.4 Summary

After a decade of experimentation, the US cyber insurance market settled on a product that addressed data breach risk primarily faced by large companies [8]. This business model was broadly profitable until as late as 2018, which can be seen in Table 2 showing that the median loss ratio among the biggest cyber insurers was just 23.4%. By the end of 2021, the ransomware epidemic had caused the median loss ratio among the biggest providers to rise to 76.9%, despite dramatic price hikes at the beginning of the year. This represents the failure of a business model that largely assessed risk via qualitative answers to questionnaires and entrusted lawyers to direct the response to cyber incidents.

Despite deteriorating loss ratios, all the insurers in Table 2 increased gross written premium in 2021. This created two new imperatives. To manage the growth, insurers needed more reinsurance and external capital to manage solvency risk. To decrease loss ratios, insurers had to solve the problems of data collection and incentives. This typically involved partnering with or acquiring InsurTech providers. Loss ratios actually stabilized in 2022 (see Table 2), although it is too early to tell whether this was caused by the insurers' improved security incentives or was instead the result of heterogeneous shocks, such as the Ukraine war impacting ransomware gangs.

The data collection elements of the insurance industry have evolved from individual, customized security audits in the early years of the cyber insurance industry, to self-reported questionnaire responses by policyholders in the data breach era, to automated scans of policyholders' networks, and most recently to integration with cloud and security vendors. Over the course of this evolution of data collection efforts it is not clear that the insurers have entirely replaced the old collection tools with new ones—or even intend to do so. For instance, many insurers that partner with cloud companies or EDR providers still require their policyholders to fill out self-reported questionnaires, even if they already have access to a large volume of security data through automated platforms. This could be in part because questionnaires help insurers to assess security governance processes that cannot be easily collected through automated platforms. It may also be because these written attestations about a company's security postures have more relevance to coverage litigation. In either case, the combination of multiple data collection methods points to how each method provides an incomplete picture in isolation. Carriers are continuing to explore better ways of collecting data about their policyholders' security and use that data to incentivize better security practices, such as the recent cloud and security vendor partnerships.

4 CYBER WARRANTIES

Cyber warranties emerged as a direct challenge to the growing cyber insurance market. At Black Hat USA 2014, Jeremiah Grossman, the founder of a security auditing firm, announced a guarantee:

> *"if a WhiteHat customer were hacked, WhiteHat would refund the customer's money for the services they paid for and the first $250,000 of any breach-related costs." [9]*

At a different conference a few months later, the pay-out was increased and Grossman described the $1.34 billion cyber insurance market as "budget left on the table" by the InfoSec industry. Grossman went on to join an end-point monitoring firm, that subsequently announced a $1 million security warranty in 2016 (W2 [57]). That year also saw two warranties (W3 [58] and W4 [59]) announced by other companies. A further 17 warranties were announced, with 15 of those in 2020 or later.

4.1 Warranties (2014—)

Coverage An express warranty is a guarantee in the contract that the product offers a certain service or level of functionality. For cyber warranties, this is typically a guarantee that it will prevent specific types of attacks linked to the functionality of the vendor's product. For example, a software auditing firm's warranty (W5) only covers losses resulting from vulnerabilities that were known at the time of audit, which means the warranty does not cover 0-day vulnerabilities [60]. A backup provider's warranty (W10) only covers encryption based ransomware incidents:

> *"a malware software program that infects Customer's systems from external sources (i.e., in the wild), which installs, persists, and encrypts a material portion of files ("Ransomware"), and continues to demand payment in order to decrypt the encrypted files." [61]*

This definition excludes ransom situations in which the criminal threatens to leak stolen data. This is admittedly justifiable given the vendor provides a cloud back-up service, which can only mitigate encryption-based threats, but it illustrates how warranties often contain idiosyncratic gaps in coverage.

Warranty terms and conditions were inconsistent [60], with coverage limits often much lower in practice than the headline announcement. For example, Rubrik announced a $5 million dollar warranty, but the small print reveals this is only available to customers who store 5 petabytes of data with the provider [61]. Those with 500 terrabytes or less received a warranty of $250k. Similarly, W2 and W12 both include a sub-limit of $1k per infected machine, which means a total of 1,000 machines would need to be infected to claim the full limit.

This narrow coverage has led various stakeholders to argue warranties do not adequately address the threat landscape [60]. A competitor of SentinelOne pointed out that their warranty only covered ransom payments to criminals and asked "couldn't SentinelOne have just offered to throw in a decent backup program?" [13]. SentinelOne responded by envisioning a world in which "a customer had endpoint security, firewalls, email security and web security, all backed by a guarantee" [13], an implicit acknowledgment that their warranty did not go far enough in isolation. A cyber insurer warned that cyber warranty "protection provided on a system by system basis could lead to confusion and inefficiencies" [14].

Solvency There is a lack of data regarding the cost of warranties in terms of pay-outs to customers, not least because these are an emerging product without the insurance industry's regulatory regime that creates reporting requirements, which allowed us to produce Table 2.[7] Some vendors offering warranties purchased insurance to manage solvency risk. For example, W9 emphasizes that their "warranty is backed by an insurance policy purchased from the Munich Re Group" [14], and W4 claims that "a top-tier insurance firm will be providing the warranty" [59].

Data Collection Vendors are unlikely to complain about the availability of technical data given they are in the business of building and operating network/device monitoring solutions. Some providers require customers to provide specific data to make a claim, such as W8 that requires "the strain of malware or data logs with associated traits for a device, and covered software affected" [65]. Most insurers do not require this level of detail to make a claim [41].

Incentives Cyber warranties are perhaps most notable for imposing onerous security requirements [60], especially relative to cyber insurance exclusions. These include a mixture of high-level requirements like "maintaining a strong cybersecurity posture" [68] and more specific procedures, such as "providing Security Awareness Training and Phishing Simulation services" [65]. The full requirements can be extensive. For example, Rurik's $5 million warranty requires completing health checks and remediating the recommendations, as well as following 'Security Hardening Best Practices'

[7] Anecdotal evidence was collected at a security conference. When an author of this paper asked about warranties at a vendor booth, the salesperson proudly claimed that their company had never paid out on their cyber warranty. This fact was meant to be a sign that their product was highly effective, even though it is implausible that none of their customers had suffered an incident given their size.

ID	Vendor	Type	Year	Limit*
W1a [9]	WhiteHatSecurity	Security audit	2014	$250k
W1b [9]	WhiteHatSecurity	Security audit	2015	$500k
W2 [57]	SentinelOne	End-point	2016	$1m
W3 [58]	MyDigitalShield	Network	2016	$50k
W4 [59]	Cymmetria	Deception	2016	$1m
W5 [62]	AsTech	Security audit	2017	$5m
W6 [63]	CrowdStrike	End-point	2018	$1m
W7 [64]	Cybereason	End-point	2020	$1m
W8 [65]	ThreatAdvice	MSP	2020	$250k
W9 [14]	Deep Instinct	End-point	2021	$3m
W10a [66]	Rubrik	Back-up	2021	$5m
W11 [67]	Arctic Wolf	MSP	2021	$1m
W12 [68]	Sophos	End-point	2022	$1m
W13 [69]	Kroll	End-point	2022	$1m
W14 [70]	Defendify	End-point	2022	$1m
W15 [71]	Dell	Back-up	2022	$10m
W10b [72]	Rubrik	Back-up	2023	$10m
W16 [73]	Veeam	Back-up	2023	$5m
W17 [74]	Barracuda	XDR	2023	?
W18 [75]	PCH Technologies	MSP	2023	?
W19 [76]	Adlumin	End-point	2023	$500k
W20 [77]	CloudCover	Network (Cloud)	2023	$1m
W21 [78]	LionGard	MSP	2023	?

Table 3. Publicly announced cyber warranties. * Many of these warranties have additional conditions (e.g. $1k per machine up to a limit of $1m) that reduce the effective limits, although this is not consistently reported.

(see Appendix A for more details). This amount of detail on security processes that must be followed was not present in cyber insurance policies in a sample from 2007 to 2017 [8].

4.2 Summary

Warranties emerged in 2014 as a challenge to the then $1.3 billion cyber insurance market [79]. Yet warranties have received constant critiques related to gaps in coverage [13, 14, 60]. These gaps help warranty providers avoid paying out on cyber attacks, thereby reducing insolvency risk. But by not paying out, the warranty providers also limit the ability of these cyber risk transfer solutions to meet customer demand for risk transfer. For this reason, warranties were a side show to the cyber insurance market that has grown rapidly since the first warranty was announced in 2014.

More positively, warranties allow vendors to differentiate themselves from competitors who are reluctant to be "liable or accountable" [80]. Warranties also provide an interesting model because of the vendors' ability to observe and influence their customers' security practices. These were two challenges that traditional insurers struggled to solve, which helped enable the ransomware epidemic.

5 PARAMETRIC INSURANCE

Parametric insurance products pay-out if predefined events occur, which can be contrasted against conventional policies that are triggered when the policyholder suffers a loss. Given parametric pay-outs are fixed ahead of time, the insurer need not investigate or quantify the harm suffered by the policyholder. Parametric triggers are often defined via externally observable events, such as a cloud outage, which are covered regardless of whether they are caused by a deliberate, malicious attack or an error.

5.1 Cloud Outage and Data Breach Cover (2019—)

Coverage The coverage of parametric insurance products varies depending on the provider. QOMPLX claimed to launch the first "multi-peril parametric insurance product" in 2019. The product provided automatic payments for small and medium-sized enterprises in the UK via three triggers: (1) the report of a data breach to the UK Information Commissioner's Office under the GDPR, (2) unplanned interruptions of "electronic services provided by a named critical partner, resulting in an outage duration of more than 48 hours," and (3) terrorism events occurring within the insured's postal code [81, 82]. The payment related to the terrorist incident is made "regardless of physical damage" [81, 82], even if the property is entirely unaffected by the incident, illustrating how parametric differs from conventional insurance. A similar parametric product for cloud outages was launched by AkinovA in 2020 [83].

In 2020, Parametrix launched parametric insurance products covering cloud service outages or downtime at named providers, including cloud providers AWS, Microsoft Azure, and Google Cloud, ecommerce platform Shopify, and content delivery networks Cloudflare, Fastly, and Akamai [84, 85]. Standard cyber insurance typically only cover losses from outages that are 8 hours or longer, whereas some Parametrix policies begin paying out just one hour after an outage begins [85]. Parametrix coverage spans many possible causes—many unrelated to security—cloud service outages:

> *"from human errors to cyber events to hardware malfunctions, including physical perils like fires, storms and hurricanes. If your provider is the target of a cyber attack and your insured cloud regions and services are impacted, you are covered."*

There are some exclusions, however, including degradation of service, planned maintenance, government and regulatory action, and war [86].

Solvency Parametric insurance providers limit their exposure to catastrophic risk through a combination of limits on policies, reinsurance, restricting new products to limited groups of customers, and exclusions for potentially large-scale risks. For instance, Parametrix's coverage limits are typically between $100,000 and $5 million but can be as high as $10 million, with payouts backed by various reinsurers [85]. Similarly, QOMPLX's WonderCover product was limited to small and medium size businesses, with limits ranging from £5,000 to £100,000 for businesses with an annual turnover of up to £12 million, and its policies were backed by a reinsurer (Chaucher) [87]. Partnerships with reinsurers are made easier by the contract certainty provided by the objective triggers associated with parametric insurance [81]. These same triggers could be used in Insurance Linked Securities (see Section 7). Finally, exclusions on events like war and regulatory action also helps limit exposure to catastrophic risk.

Data Collection In order to define a trigger, parametric providers typically need an externally verifiable method to detect whether an event has occurred. This verification method may also be used to measure the frequency of events. For example, Parametrix continuously probe popular cloud providers to detect outages. This uses external network scans rather than sensitive information about security incidents or their causes. Similarly, QOMPLX offered coverage for data breaches reported to the UK regulator under GDPR partly because there are public databases about historic breaches [88], which helps with developing actuarial models.

Incentives Parametric providers treat cyber incidents more like weather events that are out of the provider's control. For example, one provider boasts that its "policies are built on the likelihood an event will occur; the probability of occurrence is based on current and historical data, removing the uncertainty" [89], which suggests they are not actively trying to reduce the likelihood. This is justified given the likelihood is controlled by large cloud providers without any commercial relationship to the provider. However, for other triggers, such as data breaches under GDPR, the provider

could reduce the likelihood by creating incentives for improved security. Doing so is unlikely as it complicates the core selling point of parametric insurance, simplicity and certainty.

5.2 Summary

While parametric insurance provides an interesting model, it remains a niche product. For example, QOMPLX does not list the WonderCover product on its website as of February 2023 and appears to have pivoted to managed security services.[8] Growth is not helped by challenges tailoring parametric coverage to the threat landscape. As Section 3 showed, policyholders must manage the risk of a mixture of perils including ransomware, data breaches, funds transfer fraud, technology outages, media liability, and denial of service. Parametric products cover at best one or two of these risks, which necessitates finding alternative solutions for the others. It also requires firms to know ahead of time how much an incident will cost—over-estimating potential costs leads to unnecessarily expensive products (although this represents a windfall if the event occurs), while policyholders must accept the residual risk that costs were under-estimated.

More positively, parametric insurance avoided the challenge conventional cyber insurance providers face in lacking reliable data about cybersecurity incidents. Parametric pricing need not estimate the damage associated with events, and can instead focus on the frequency of specific events, which can often be externally measured. This allows providers to largely ignore the challenge of incentivizing more secure behavior. Simplicity also speeds up claims processing as the pay-out is fixed. QOMPLX touts its "automatic payments based on objective triggers" and the fact that its policyholders "receive payment quickly rather than waiting to find out if a claim qualifies or enduring a potentially contentious loss adjustment process" [81, 87].

6 REINSURANCE

In describing the main primary risk transfer products (cyber insurance, cyber warranties and parametric insurance), we found that all relied on reinsurers to manage solvency. This helps to explain how reinsurers hold so much cyber risk. Insurers were ceding 46% of cyber premiums to reinsurers as of January 2021, up from 40% in 2020 [90]. Despite the size of the cyber reinsurance market, there is a dearth of academic research.

6.1 Quota Share (2000s—)

Coverage Reinsurers can extend coverage for cyber losses via two broad mechanisms: (i) silent cyber in which via non-cyber policies; (ii) affirmative cyber reinsurance. Typically reinsurance contracts do not specify which specific losses are covered because this is inherited from the wordings of the primary policies. Nevertheless, the structure of the different types of reinsurance are worth discussing.

Silent cyber coverage is defined to be "implicit cyber exposure within 'all risks' and other liability insurance policies that do not explicitly exclude cyber risks" [91]. This means traditional reinsurance may cover cyber losses, even if the (re)insurers did not expect this. The industry and regulatory community have been aware of this issue since at least 2012 [92]. In 2020, Wrede et al. [93] analyzed 48 traditional insurance policies and interviewed 10 practitioners and discover "a considerable amount of silent cyber coverage" in the German market.

The most common type of affirmative cyber reinsurance is *quota share*, which represented 95% of all cyber reinsurance in 2017 [34]. Quota share reinsurance is typical of immature markets [94]. In a quota share agreement, claims costs are shared between insurer and reinsurer in a fixed proportion (e.g. 50-50).

[8] https://www.qomplx.com/about-qomplx/

Another type of reinsurance is *excess of loss* (XoL) reinsurance, in which reinsurers only pay if claims exceed a defined threshold. Depending on the limits and deductibles, this means reinsurers pay a greater fraction of claims when extreme losses occur, but insurers pay a greater share of claims in typical years. Reinsurers are reluctant to accept this structure in cyber insurance because of uncertainty about the potential for catastrophic losses [95]. Nevertheless, the prevalence of XoL treaties has increased since 2017 [96].

Solvency The market concentration in cyber insurance is extreme given half of all cyber premiums ultimately flow to reinsurers [50, 90]. One industry insider reports that "the four largest reinsurers of affirmative cyber represent close to 80 per cent of the total market" [97]. There is an order of magnitude more cyber insurers who collectively represent the other half of cyber premiums [98]. While this concentration of risk is concerning, it is worth noting that quota share arrangements have a cap on the reinsurer's loss ratio (e.g. 400%), which limits catastrophic exposure for the reinsurer. Reinsurers further manage insolvency by writing multiple lines of insurance, being well-capitalized and purchasing retrocession policies (insurance for reinsurers).[9] Reinsurers can also offload catastrophe risk to capital markets [96], something we consider in the next section.

While reinsurers are actively managing their exposure to affirmative cyber reinsurance, it is harder to track their exposure to silent cyber. The NotPetya cyber attack provides a useful case study because the White House estimated it caused $10 billion of damage. Only $3 billion of those losses were insured [99], of which just $300 million was claimed under a policy that affirmatively covered cyber. The proportion of affirmative to silent cyber claims (1:9) is notable. Extrapolating from this case-study is complicated by ongoing efforts to eradicate silent cyber coverage and also the relatively higher limits available for non-affirmative coverage. Regardless of the distribution across silent and affirmative reinsurance, the worst cyber loss in recent history (NotPetya at $10 billion) is an order of magnitude smaller than the worst natural catastrophes, such as Hurricane Ian at $113 billion [96].

Data Collection Whereas insurers are limited to their customer base, reinsurers can collect information about claims, policy language, and risk assessments from all of the primary insurers who purchase reinsurance. This data could be aggregated across all of the quota share agreements (covering 50% of premiums), eventually creating a data repository. Reinsurers thereby create claims repositories—a long standing public-policy goal [92]—via normal business operations. In collecting this data, reinsurers are limited by problems related to unstructured data collected without a common data schema [92] and also litigation risk distorting claims reports [54]. The resulting uncertainty, in particular the lack of consensus on risk distributions, may be limiting growth in cyber reinsurance and the wider market [100]. Exploring this issue provides an interesting avenue for future work.

Incentives Quota share contracts primarily limit principal-agent issues because primary insurers have a proportional exposure to catastrophe [24], unlike under an XoL treaty. Reinsurers also audit the primary insurer's underwriting and claims history during the application process. Primary insurers can negotiate better deals if they show more due diligence and expertise when underwriting. The proportion (50%) of premiums that flow to cyber reinsurers suggests they have significant market power, although the lack of research means it is unclear how this is wielded. Anecdotal reports suggest a major reinsurer took the "necessary steps" to ensure its primary insurance customers included a sufficiently broad cyber war exclusion [101].

[9] It is unclear who the biggest reinsurers can buy retrocession from, given they already represent the vast majority of the cyber reinsurance market.

6.2 Summary

Quota reinsurance allowed primary insurers to de-load risk, both catastrophic and typical, but also meant profit was shared with reinsurers. The limited growth of XoL policies meant that reinsurers shared the exposure to catastrophic risk with insurers. By 2022, a small number of reinsurers sold the majority of cyber reinsurance. This is partly because the other reinsurers were uncomfortable with cyber risk, but also due to "instances of deliberate aggressive growth among the top four" [96].

As the market concentration peaked, primary insurers began to seek alternatives to cyber reinsurance. For large multi-line insurers, more self-insurance is an option. This may explain why the largest US cyber insurer canceled their cyber reinsurance treaty in 2023 [102], given their cyber business is a fraction of the firm's total business. The insurer, along with others, opted instead to tap capital markets. As the next section outlines, these solutions ranged from insurers issuing cat bonds through to an InsurTech firm founding its own reinsurer.

7 CAPITAL MARKETS

The capacity crunch in reinsurance markets increased demand for alternatives. That predominantly involves transferring risk to investors.

7.1 Insurance Linked Securities (2022—)

Coverage The most important ILS product is a cat bond. Cat bonds function like normal bonds if there is no catastrophe, in that investors receive their initial investment (the principal) plus a stream of interest payments.[10] The main difference is that cat bonds forgive the repayment of interest and (some of) the principal if a catastrophe arises. The issuer, the (re)insurer, can use the freed up funds to cover claims related to the catastrophe. As such, cat bonds must clearly define the conditions describing the covered catastrophic events. These triggers can be divided into indemnity triggers based on underwriting losses, and parametric triggers based on externally observable events.

Cyber cat bonds were slow to develop. The first cat bond that explicitly covered cyber risk was issued by Credit Suisse in 2016. The trigger focused on operational risk, with cyber representing just one potential exposure among many [103].[11] The first standalone cyber cat bond was issued in 2023 [10]. It provides one year of per-occurrence indemnity reinsurance protection against a "remote probability catastrophic and systemic events" [104]. Table 4 shows other insurers followed by issuing their own cat bonds. All of these bonds include triggers based on insured losses exceeding a certain threshold, not a parametric trigger like an outage at a particular cloud provider. SwissRe's Cat Bond differs slightly in that it is triggered by losses across the entire US cyber industry exceeding a threshold of $9 billion, not just losses in SwissRe's portfolio [105].

Alternative structures were used by HannoverRe and Coalition to raise $100m and $300m respectively from capital markets. HannoverRe issued a quota share arrangement, by which investors share reinsurance losses on a proportional basis (similar to when insurers purchase quota share reinsurance). Coalition secured $300m from a range of investors in order to launch an independent reinsurer [106], which could then sell reinsurance to Coalition.

[10]The principal is typically returned three to five years later. The investors' funds may be held in a secure collateral account. In exchange for assuming the risk of losing the principal, cat bonds have a higher yield than conventional bonds (e.g. 15%) with the exact value determined by the likelihood of the specified catastrophe.

[11]The bond covers "exposures including: certain cyber risk exposures, such as IT system failure that causes business interruption; fraudulent behaviour both of external parties and employees of the investment bank; fiduciary issues; losses due to improper business practices or unauthorised activity; accounting errors; documentation errors; regulatory compliance issues; HR issues; discrimination in the workplace; or even personal injury."

Cedant	Trigger	Type	Size	Date
Beazley	Indemnity	Private Cat Bond	$45m	Jan 2023
HannoverRe	Indemnity	Quota share retrocession	$100m	Jan 2023
Beazley	Indemnity	Private Cat Bond	$20m	May 2023
Beazley	Indemnity	Private Cat Bond	$16.5m	Sep 2023
AXIS Capital	Indemnity	Cat Bond (144A)	$75m	Nov 2023
Beazley	Indemnity	Cat Bond (144A)	$130m	Dec 2023
SwissRe	Indemnity*	Cat Bond (144A)	$50m	Dec 2023
Chubb	Indemnity	Cat Bond (144A)	$100m	Dec 2023

Table 4. Cyber insurers transfer risk to capital markets using a range of solutions. * the first cyber cat bond with an industry loss index trigger.

Solvency The first cyber cat bond was just $45 million [10], which is dwarfed by the wider market for natural catastrophe bonds that was estimated to be $38.2 billion in June 2022 [107]. Similarly, the $300m investment in establishing a reinsurer is a fraction of that private equity firm's total investments [106], let alone the wider market. This diversification is a core attraction of capital markets. It is implausible that cyber risk transfer products could destabilize capital markets because the sums of money at play are too small, even if the cat bond limits were totally exhausted. However, losses are likely to reduce the supply of cat bonds in subsequent years, which creates capacity issues for (re)insurers.

Data Collection Much like reinsurers, the reliance on indemnity triggers mean investors must model not only the likelihood of catastrophe, but also how the event would translate into insured losses. To do this, investors must assess the underwriting quality of their (re)insurance partners for quota share agreements. For example, an investor can only evaluate the value of a cat bond with an indemnity trigger by understanding how likely it is that the issuer's cyber portfolio results in a qualifying loss. This requires the cooperation of the issuer, which involves sharing details on underwriting strategy and historic performance.

This is different for parametric triggers, in which cat bond payouts are determined by a so-called objective trigger. For example, a cyber cat bond might pay-out if there was an outage of at least 36 hours at 3 or more regional data centers at the main cloud providers in the USA. To evaluate such a bond, investors would need to model cloud outages, much like Parametrix do at present. The lack of reliable cyber cat models, as well as basis risk, is part of why we are likely to see quota share/indemnity trigger mechanisms for the foreseeable future.

Incentives We are not aware of any articles explaining how capital markets influence the day-to-day operations of either reinsurers, insurers, or risk holders. However, one can imagine the potential for this. In a speculative essay, Bruschi [108] describes how cyber cat bonds could disincentivize states launching cyber attacks against each other. He suggests that if Russia held cyber bonds issued by the US insurance industry then "Vladimir Putin would have to worry [before launching an attack] about erasing billions of dollars from his own country's pension funds, possibly leading to riots in the streets" [108]. A similarly outlandish scenario is that an ILS investor requires insurers to no longer write a certain industry or avoiding specific technologies. This is unlikely given ILS products are sold to a range of investors, who manage a portfolio of ILS investments.

An evolutionary mechanism seems more realistic. Rational markets would offer the capital most willingly to those insurers who can demonstrate superior underwriting processes. Cheap capital allows those insurers to expand

underwriting. This could improve social welfare if capital markets reward insurers who actively improve the security posture of policyholders, as imagined by early articles on cyber insurance [22].

7.2 Summary

Experiments in transferring cyber risk to capital markets are the newest development covered in this paper. The size of the investments remains modest, which reflects the huge uncertainty involved. For example, the initial $45 million cyber cat bond is a drop in the ocean of the larger cat bond market. However, further tranches were subsequently issued. This cat bond model defined via an indemnity trigger based on the primary insurers' cyber claims is a simple structure. Coalition securing $300 million to create an independent reinsurer provides an alternative model [106]. Another interesting model is a parametric trigger linked to a specific event.

8 DISCUSSION

This section aims to distill the core themes emerging from the five risk transfer products. This resulted in the following high-level research goals, which we describe in more detail in the following:

(1) Develop a suite of parametric triggers that cover the threat landscape and address basis risk.
(2) Advance state-of-the-art cyber catastrophe models to understand exposure to aggregate risk.
(3) Quantify internal security to better model and price security processes.
(4) Define and enforce a standard of reasonable security based on statistical evidence.

Indemnity Coverage is King Indemnity based cyber (re)insurance products were the most successful in terms of market growth. This can be seen in the combined markets for primary cyber and quota share cyber reinsurance hitting $10 billion. These products were flexible enough to cover the threat landscape as it shifted away from data breaches towards ransomware and funds transfer fraud. A more recent example is the spike in lawsuits related to unlawful web tracking, for which "there's cover under many cyber policies" [109]. Reinsurance covers these claims unless the reinsurer has proactively excluded that peril, which is rare.

In contrast, parametric products cannot easily adjust to the threat landscape. For example, the QOMPLX product paid out if a policyholder reported a data breach to the regulator. The policy would not be triggered if the ransomware gang did not exfiltrate data following an incident, even though the firm might still face a sizable ransom demand and business interruption loss. The solution is to define better triggers, in particular a suite of parametric triggers that cover the full spectrum of cyber losses.

Dal [110] proposed a parametric trigger based on a threshold of activity from a commercial threat intelligence feed. This is analogous to natural catastrophe triggers defined in terms of the strength of a wind storm or earthquake on a scientific scale. It remains unclear whether threat intelligence activity proxies insurance claims, again the problem of basis risk. In contrast, Parametrix's product directly hedges the risk of cloud outages because the trigger includes both malicious and accidental causes. To build on this, researchers should work on developing parametric triggers that: (i) are objective; (ii) reliably proxy digital losses; and (iii) are externally verifiable.

Aggregation Models The capital crunch, in which primary insurers are scrambling to find efficient solutions to hedge catastrophic risk, emerged around 2021. This is perhaps strange given that cyber has avoided catastrophic outcomes, thus far at least [111]. The core problem is a lack of trust in cyber catastrophe models. In comparison to nat cat models of hurricanes and winter storms, market-leading cyber cat models display "an extended tail and a high

degree of uncertainty" [112]. The heavy tail is partly driven by conservative assumptions, such as not taking into account that cloud services comprise geographically diversified data centers [113].

The challenge for future researchers is to accurately model the potential for cyber catastrophe. This will require multiple models that can account for how different perils arise. Cloud outages are caused by a centralized entity failing to prevent the incident, whereas wormable malware results from multiple insureds failing to prevent the incident. Even worse, distributed Denial of Service attacks can be caused by uninsured entities failing to prevent botnet infection. Large scale casualty losses are caused by trends in the legal system, such as recent court cases about whether web tracking violates the 1988 Video Privacy Protection Act [109]. Given how quickly the threat landscape changes, each of the four scenarios could be the cause of the first cyber catastrophe, or it could be the result of an as-yet-unimagined scenario. The science of cyber cat modelling must address these unknowns.

Quantifying Internal Security The rise of InsurTech firms relied on using external network scans for underwriting. Some carriers subscribed to a scanning platform, meanwhile others acquired or built these capabilities. Network scans provide externally verifiable security information, providing the relevant IP range is identified. However, external scans cannot collect data about internal IT infrastructure, let alone processes or the awareness of employees.

This leads to the research challenge of collecting more information about internal assets and security culture. The former could involve asset discovery techniques deployed from within the network, or alternatively making inferences based on external indicators [114]. Measuring security awareness is an ongoing area within Human-Computer Interaction [115, 116]. However, any data collection techniques must be sufficiently light-weight so as not to increase friction when purchasing risk transfer products. This is perhaps why insurers have partnered with technology vendors who already have network access, as in the cloud and security vendor partnerships. Even so, cloud providers may still have to figure out how to make their customers' data accessible and comprehensible to an insurer.

As insurers have wrestled with data collection, many regulators have also taken an interest in trying to collect more data about cybersecurity incidents through regulatory reporting schemes. Such efforts include the Securities and Exchange Commission cybersecurity disclosure rules, the Cyber Incident for Critical Infrastructure Reporting Act of 2022, and the European Union's NIS2 Directive. While it is still unclear whether the data collected by regulators under these programs will be useful to insurers and others engaged in cyber risk transfer, it is notable that government stakeholders are also concerned with the lack of reliable data about cyber risk and are taking steps to address the problem.

Defining Reasonable Security Creating incentives to improve security requires finding a balance. If providers require too much security, then policyholders will fail to meet achieve it, pay-outs will be denied, and trust in the risk transfer product will fall—we suggested this was the case for many cyber warranties. If the required security level is too low, then pay-outs will be frequent and providers will be forced to raise the price of the product—we suggested this was the case for cyber insurance as it transitioned from the data breach to ransomware era. Thus, a major challenge is to define and enforce reasonable security. This is also an area where regulators are increasingly active in trying to determine baseline expectations and standards for cybersecurity.

Realistically, there is no single definition, but instead a range of contextual definitions. This can be seen in the warranty T&Cs that were tailored to the functionality of each product. One option would be to require the most effective security controls, although the state of the scientific literature was underwhelming in 2021 [21]. An interesting direction is to instead seek to understand societal expectations around security [117].

Alternative Histories Finally, we turn to the accuracy and completeness of our study. We titled our article as 'a history' instead of 'the history' to invite authors to publish alternative histories of individual products or cyber risk

transfer at large. At best, our work sketched the high-level development of these products in terms of which perils are covered, what data is collected, and who partners with who. Future work is undoubtedly needed to fill in details, such as how policy wordings developed over time.[12] At worst, our account does not represent the broad history as seen by others. We encourage authors to come forward to address both issues.

Most fundamentally, cyber risk transfer products continue to evolve at a rapid pace. Professional historians typically wait decades before beginning historical research, meanwhile we waited months for some sections.[13] We have no doubt that the cyber risk transfer landscape will look completely different in a decade, and look forward to reading future works on those differences.

9 CONCLUSION

Cyber risk transfer mechanisms adopt diverse approaches to solving the challenges of coverage, solvency, data collection, and incentives. The growth of cyber risk transfer is a challenge to the cybersecurity industry. The first warranty was announced at a prestigious InfoSec conference, with the speaker arguing the then $1.4bn cyber insurance industry was "budget left on the table" by InfoSec vendors [79]. In the following decade, tens of InfoSec vendors announced warranties (see Table 3). Due to gaps in coverage, warranties failed to displace the cyber insurance market, which grew by over 1000%.

In contrast, insurers seek first to offer broad coverage, and then scramble to measure and incentivize risk prevention across the diverse perils. In contrast, warranties and parametric insurance offer a cyber risk transfer solution for a narrow set of risks for which the provider has significant visibility, leaving the customer to manage the uncovered risks. For this reason, indemnity insurance became the mainstream cyber risk transfer mechanism.

As the market grew in size, the challenge of obtaining external capital became difficult due to the cyber reinsurance capacity crunch. To continue growing their portfolio, a number of primary insurers transferred risk to investors. To date, the most common schemes to secure capital are defined in terms of the primary insurer's claims. This is clearly true of quota share reinsurance, the most common approach, but it is also true of the first cat bonds (see Table 4). We are yet to see capital investors rely on parametric triggers, in which pay-outs are determined by an externally verifiable event. Though parametric insurance providers are experimenting with small sums, the triggers could still be re-used for by capital investors. Any risk that cannot be off-loaded to reinsurers or capital markets will be held by the primary insurer, with the insurer holding a greater share of the rewards.

Despite this growth, Schneier's prophecy that "the computer security industry will be run by the insurance industry" has not yet come to pass [22]. A step in the opposite direction sees cloud and security vendors define the APIs through which cyber risk information is communicated. In this model, insurers improve data collection by partnering with technology firms. Another model sees insurers harness technology, such as buying scans as a service or acquiring cyber technology firms [41, 43]. Yet another model is provided by InsurTechs who first build a technology platform and then later solve the insurance problems by, for instance, securing venture/private capital to establish independent insurance and reinsurance companies [106, 118]. The coming years will see which model is superior, and whether InfoSec warranties, parametric insurance, or an as-yet-unknown disrupter can mount a late challenge.

[12] For example, Michael Rossi uploaded a document titled "An Abbreviated History of Cyber Insurance - The First Twenty Five Years" to LinkedIn in March 2024. This document described his personal experiences negotiating coverage for clients purchasing cyber insurance. His account is broadly similar to Section 3 in that cyber insurance evolved from an experimental stage to a third-party privacy risk stage to a ransomware stage. Rossi is more focused on the buyers of risk transfer products, such as the need to satisfy contractual requirements to have cyber insurance coverage and the extent to which IT departments cooperated in the buying process.

[13] Our first draft of this article was completed at the end of 2022. Since then, we revised different parts as academic articles were published and new announcements were made.

ACKNOWLEDGEMENTS

We received insightful feedback on this paper from Dan Schwarcz, Monica Shokrai, Peter Wedge, and Tom Johansmeyer. We also received two useful rounds of feedback from submitting to WEIS'23, where we presented a poster, and WEIS'24.

REFERENCES

[1] Bob Blakley, Ellen McDermott, and Dan Geer. Information security is information risk management. In *Proc. of the 2001 Workshop on New Security Paradigms*, pages 97–104. ACM, 2001.

[2] Lawrence A Gordon, Martin P Loeb, and Tashfeen Sohail. A framework for using insurance for cyber-risk management. *Communications of the ACM*, 46(3):81–85, 2003.

[3] Lawrence D Bodin, Lawrence A Gordon, and Martin P Loeb. Information security and risk management. *Communications of the ACM*, 51(4):64–68, 2008.

[4] Martin Eling, Michael McShane, and Trung Nguyen. Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, 24(1):93–125, 2021.

[5] Sasha Romanosky and Elizabeth Petrun-Sayers. Enterprise risk management: how do firms integrate cyber risk? *Management Research Review*, 47(1):1–17, 2023.

[6] Carl E Landwehr. Computer security. *International Journal of Information Security*, 1(1):3–13, 2001.

[7] Josephine Wolff. *Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks*. MIT Press, 2022.

[8] 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.

[9] Sean Michael Kerner. Whitehat is guaranteeing security. *eWeek*, 2015. Accessed: 2023-02-7.

[10] Ian Smith. Insurer Beazley launches first catastrophe bond for cyber threats. *Financial Times*, 2023. Accessed: 2023-02-8.

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

[12] Ross Anderson and Tyler Moore. The economics of information security. *Science*, 314(5799):610–613, 2006.

[13] John Leyden. Sentinelone's $1m ransomware guarantee dismissed as pr stunt. *The Register*, 2016. Accessed: 2023-02-7.

[14] Steve Zurier. Deep Instinct to offer $3 million ransomware warranty. *SC Media*, 2021. Accessed: 2023-02-7.

[15] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Carlos Ganán, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. Measuring the changing cost of cybercrime. In *Workshop on the Economics of Information Security*, 2019.

[16] Ross Anderson, Rainer Böhme, Richard Clayton, and Ben Collier. Silicon den: Cybercrime is entrepreneurship. In *Workshop on the Economics of Information Security (WEIS)*, 2021.

[17] Rainer Böhme and Gaurav Kataria. Models and measures for correlation in cyber-insurance. In *Workshop on the Economics of Information Security*, 2006.

[18] Dan Geer, Eric Jardine, and Eireann Leverett. On market concentration and cybersecurity risk. *Journal of Cyber Policy*, pages 1–21, 2020.

[19] Gregory Falco, Martin Eling, Danielle Jablanski, Matthias Weber, Virginia Miller, Lawrence A Gordon, Shaun Shuxun Wang, Joan Schmit, Russell Thomas, Mauro Elvedi, et al. Cyber risk research impeded by disciplinary barriers. *Science*, 366(6469):1066–1069, 2019.

[20] Stefan Laube and Rainer Böhme. The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity*, 2(1):29–41, 2016.

[21] Daniel W. Woods and Rainer Böhme. SoK: Quantifying cyber risk. In *IEEE Symposium on Security and Privacy*, pages 909–926, Oakland, CA, May 2021.

[22] Bruce Schneier. Insurance and the computer industry. *Communications of the ACM*, 44(3):114–114, 2001.

[23] Rainer Böhme and Galina Schwartz. Modeling cyber-insurance: Towards a unifying framework. In *Workshop on the Economics of Information Security*, 2010.

[24] Rob Thoyts. *Insurance theory and practice*. Routledge, 2010.

[25] Philip Booth, Robert Chadburn, Steven Haberman, Dewi James, Zaki Khorasanee, Robert H Plumb, and Ben Rickayzen. *Modern actuarial theory and practice*. CRC Press, 2020.

[26] Tom Baker. Back to the future of cyber insurance. *Professional Liability Underwriting Society*, 3(1):5–6, 2019.

[27] Ty Sagalow. On making lemonade. *Not Unreasonable Podcast*, 1(41), 2019.

Disclosure Statement Our first draft was written before the first author, Daniel Woods, took up employment at Coalition, who are an active participant in the cyber insurance market. Revisions were undertaken since this employment commenced, but the main structure and conclusions of the article are unchanged. The views and opinions expressed as part of this paper are solely those of Daniel Woods in a scholastic capacity, and do not necessarily state or reflect those of Coalition. Neither Coalition nor any of its employees make any warranty of any kind, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product or process disclosed. This article is designed to provide general information on the topic presented and is not intended to construe or the rendering of legal or other professional services of any kind.

[28] Sasha Romanosky, Rahul Telang, and Alessandro Acquisti. Do data breach disclosure laws reduce identity theft? In *Workshop on the Economics of Information Security*, 2008.

[29] Josephine Wolff. *You'll See This Message When It Is Too Late: The Legal and Economic Aftermath of Cybersecurity Breaches*. MIT Press, 2018.

[30] Verizon. 2016 Data Breach Investigations Report: Available: https://conferences.law.stanford.edu/cyberday/wp-content/uploads/sites/10/2016/10/2b_Verizon_Data-Breach-Investigations-Report_2016_Report_en_xg.pdf, 2016. [Online; accessed 11-Feb-2023].

[31] Spencer Wheatley, Thomas Maillart, and Didier Sornette. The extreme risk of personal data breaches and the erosion of privacy. *The European Physical Journal B*, 89(1):7, 2016.

[32] Nicole Perlroth and Elizabeth A. Harris. Cyberattack insurance a challenge for business. *The New York Times*, 2014.

[33] Judy Greenwald. Target data breach prompts insurers to scale back cyber coverage for retailers. *Business Insurance*, 2014.

[34] Scor. State of the cyber (re)insurance market. https://www.scor.com/en/files/state-cyber-reinsurance-market, 2017.

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

[36] Daniel W Woods, Tyler Moore, and Andrew C Simpson. The county fair cyber loss distribution: Drawing inference from insurance prices. In *Workshop on the Economics of Information Security*, 2019.

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

[38] Jamie MacColl, Jason RC Nurse, and James Sullivan. Cyber insurance and the cyber security challenge. *Royal United Services Institute Occasional Paper Series*, 2021. [Online; accessed 19-Sep-2022].

[39] Shauhin A Talesh and Bryan Cunningham. The technologization of insurance: An empirical analysis of big data and artificial intelligence's impact on cybersecurity and privacy. *Utah Law Review*, 2021.

[40] Josephine Wolff and William Lehr. Roles for policy-makers in emerging cyber insurance industry partnerships. 46th Research Conference on Communication, Information and Internet Policy, 2018.

[41] Daniel W. Woods and Rainer Böhme. How cyber insurance shapes incident response: A mixed methods study. In *Workshop on the Economics of Information Security*, 2021.

[42] Staff Writers. Arch to back coalition cyber insurance programs with long-term capacity. *Insurance Journal*, 2021. Accessed: 2023-02-8.

[43] Saumya Jain. Travelers expands cyber capabilities with acquisition of corvus insurance. https://www.reinsurancene.ws/travelers-expands-cyber-capabilities-with-acquisition-of-corvus-insurance/, 2023.

[44] CNW Group. Chubb and sentinelone partner to enhance cyber risk management. *Yahoo Finance*, 2023.

[45] Microsoft News Center. Microsoft and At-Bay partner to offer data-driven cyber insurance coverage Available: https://news.microsoft.com/2021/09/29/microsoft-and-at-bay-partner-to-offer-data-driven-cyber-insurance-coverage/, 2021. [Online; accessed 5-Feb-2023].

[46] Cowbell. Cowbell and Swiss Re Partner to Offer First Ever Cyber Insurance Program Dedicated to Cloud Workloads: Available: https://cowbell.insure/news-events/pr/cowbell-and-swiss-re-partner-on-cyber-insurance-for-cloud/, 2022. [Online; accessed 11-Feb-2023].

[47] Google. Risk Protection Program Preview Available: https://cloud.google.com/risk-protection-program, 2021. [Online; accessed 5-Feb-2023].

[48] Andrew Coburn, Eireann Leverett, and Gordon Woo. *Solving Cyber Risk: Protecting Your Company and Society*. Wiley, 2018.

[49] PricewaterhouseCoopers. Are insurers adequately balancing risk & opportunity? findings findings from pwc's global cyber insurance survey. https://www.pwc.com/us/en/industry/assets/pwc-cyber-insurance-survey.pdf, 2018.

[50] Anthony Cordonnier. Cyber reinsurance in the "new normal". https://www.swissre.com/reinsurance/property-and-casualty/reinsurance/casualty-reinsurance-underwriting/cyber-reinsurance-in-the-new-normal.html, 2020.

[51] Samaneh Tajalizadehkhoob, Tom Van Goethem, Maciej Korczyński, Arman Noroozian, Rainer Böhme, Tyler Moore, Wouter Joosen, and Michel van Eeten. Herding vulnerable cats: A statistical approach to disentangle joint responsibility for web security in shared hosting. In *Proc. of the Conf. on Computer and Communications Security*, pages 553–567. ACM, 2017.

[52] Adam Tyra. Ranking email security solutions a data analysis of cyber insurance claims. https://www.at-bay.com/ranking-email-security-solutions, 2023. Accessed: 2023-02-27.

[53] Allianz and MunichRE. Cloud Protection + Innovative Cyber Solutions for Google Cloud Customers Fact Sheet Available: https://www.cloud-protection-plus.com/content/dam/munichre/mrwebsitescpp/Allianz-NA-Google-Cloud-Protection-Sales-Sheet.pdf/_jcr_content/renditions/original./Allianz-NA-Google-Cloud-Protection-Sales-Sheet.pdf, 2021. [Online; accessed 5-Feb-2023].

[54] Daniel Schwarcz, Josephine Wolff, and Daniel W Woods. How privilege undermines cybersecurity. *Harvard Journal of Law & Technology*, 2023 (forthcoming).

[55] 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.

[56] 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.

[57] Lindsay Ciulla. Sentinelone establishes $1 million cyber threat protection warranty giving first-ever industry assurance against growing threats. https://www.sentinelone.com/press/sentinelone-establishes-1-million-cyber-threat-protection-guarantee/, 2016. Accessed: 2023-02-7.

[58] Robert Byrd and Michiko Morales. Assurant partners with mydigitalshield to offer small businesses protection against data breaches. https://www.assurant.com/newsroom-detail/NewsReleases/2016/June/Assurant-Partners-with-MyDigitalShield-to-Offer-Ticker-Businesses-Protection-against-Data-Breaches, 2016. Accessed: 2023-02-7.

[59] Nathaniel Mott. Cymmetria offers $1m warranty to make cybersecurity more accountable. *Tom's Hardware*, 2016. Accessed: 2023-02-7.

[60] Daniel W Woods and Tyler Moore. Cyber warranties: market fix or marketing trick? *Communications of the ACM*, 63(4):104–107, 2020.

[61] Rubrik, Inc. Rubrik enterprise edition ransomware recovery warranty agreement. https://www.rubrik.com/content/dam/rubrik/en/resources/policy/rubrik-enterprise-edition-ransomware-recovery-warranty-agreement.pdf, 2022. Accessed: 2023-02-7.

[62] Dark Reading Staff. Astech offers a $5 million security breach warranty. *Dark Reading*, 2017. Accessed: 2023-02-7.

[63] Catalin Cimpanu. Crowdstrike to pay up to $1 million warranty if its clients suffer a data breach. *Bleeping Computer*, 2018. Accessed: 2023-02-7.

[64] Sabina Reghellin. Cybereason announces $1 million comprehensive breach protection warranty. *IT Security Guru*, 2020. Accessed: 2023-02-7.

[65] ThreatAdvice. Threatadvice breach prevention warranty. https://www.threatadvice.com/warranty, 2020. Accessed: 2023-02-7.

[66] Chris Mellor. Up to $5m compensation if rubrik cloud vault recovery busted. *Blocks & Files*, 2022. Accessed: 2023-02-7.

[67] Arctic Wolf. Arctic wolf backs security operations portfolio with $1 million service assurance benefit. https://arcticwolf.com/resources/press-releases/arctic-wolf-backs-security-operations-portfolio-with-1-million-service-assurance-benefit/, 2021. Accessed: 2023-02-27.

[68] Rob Harrison. Introducing the sophos breach protection warranty. https://news.sophos.com/en-us/2022/11/30/introducing-the-sophos-breach-protection-warranty/, 2022. Accessed: 2023-02-7.

[69] Devonne Cusi and Lindsey Challis. Kroll adds complimentary $1 million incident protection warranty to managed detection and response (mdr) service. *Business Wire*, 2022. Accessed: 2023-02-7.

[70] Defendify. Defendify launches $1 million cybersecurity service warranty to insulate organizations financially from the damages of cyber threats. https://www.defendify.com/newsroom/defendify-launches-1-million-cybersecurity-service-warranty-to-insulate-organizations-financially-from-the-damages-of-cyber-threats/, 2022. Accessed: 2023-11-7.

[71] Dell. Dell delivers cyber recovery guarantee. https://www.dell.com/en-us/blog/dell-delivers-cyber-recovery-guarantee/, 2023. Accessed: 2023-11-7.

[72] Rubrik. Rubrik ups the ante with $10 million ransomware recovery warranty. https://www.rubrik.com/company/newsroom/press-releases/23/rubrik-ups-the-ante-with-10-million-ransomware-recovery-warranty, 2023. Accessed: 2023-11-7.

[73] Veeam. Veeam ransomware recovery warranty veeam has you covered. https://www.veeam.com/products/ransomware-recovery-warranty.html, 2023. Accessed: 2023-02-27.

[74] Barracuda. Barracuda partners with cork to offer cyber warranty created exclusively for customers of msps. https://www.prnewswire.com/news-releases/barracuda-partners-with-cork-to-offer-cyber-warranty-created-exclusively-for-customers-of-msps-301895061.html, 2023. Accessed: 2023-11-7.

[75] Business Wire. Pch technologies launches cyber warranty program for small business clients, powered by corktm. *Yahoo Finance*, 2023. Accessed: 2023-11-7.

[76] Adlumin. Adlumin unveils warranty and cyber insurance offerings that make coverage attainable and affordable for previously unprotected small and mid-sized organizations. https://adlumin.com/news/press-release/adlumin-unveils-warranty-and-cyber-insurance-offerings/, 2023. Accessed: 2023-11-7.

[77] Kassandra Jimenez-Sanchez. Munich re and cloudcover announce partnership. *Reinsurance News*, 2023. Accessed: 2023-11-7.

[78] Bruce Christian. Cork cyber warranty becomes available through liongard msp partners. https://channelvisionmag.com/cork-cyber-warranty-becomes-available-through-liongard-msp-partners/, 2023. Accessed: 2023-11-16.

[79] Jeremiah Grossman. No More Snake Oil: Why InfoSec Needs Security Guarantees Available: https://www.slideshare.net/jeremiahgrossman/no-more-snake-oil-why-infosec-needs-security-guarantees, 2015. [Online; accessed 27-Feb-2023].

[80] Kelly Sheridan. Cyber warranties: What to know, what to ask. *Dark Reading*, 2018. Accessed: 2023-02-7.

[81] Evans, Steve. QOMPLX & Chaucer launch multi-peril parametric insurance for SME's: Available: https://www.artemis.bm/news/qomplx-chaucer-launch-multi-peril-parametric-insurance-for-smes/, 2019. [Online; accessed 11-Feb-2023].

[82] QOMPLX. QOMPLX and Chaucer Launch First-Ever Parametric Multi-Peril Insurance Product for Small-to-Medium Enterprises: Available: https://https://www.qomplx.com/qomplx-and-chaucer-launch-first-ever-parametric-multi-peril-insurance-product-for-small-to-medium-enterprises/, 2019. [Online; accessed 11-Feb-2023].

[83] Evans, Steve. Parametric cloud outage cyber risk transfer deal backed by Hiscox: Available: https://www.artemis.bm/news/parametric-cloud-outage-cyber-risk-transfer-deal-backed-by-hiscox/, 2020. [Online; accessed 11-Feb-2023].

[84] L.S. Howard. How cloud downtime insurance became a thing. *Insurance Journal*, 2022.

[85] John McCormick. Startup sells insurance coverage for cloud outages. *The Wall Street Journal*, 2022.

[86] Parametrix Insurance. Downtime Insurance for Cloud Services Available: https://parametrixinsurance.com/cloud/, 2022. [Online; accessed 5-Feb-2023].

[87] QOMPLX. QOMPLX: Protection for Small Businesses: Available: https://go.qomplx.com/rs/449-EVP-026/images/insurance-wondercover-datasheet.pdf, 2020. [Online; accessed 11-Feb-2023].

[88] Josephine Wolff and Nicole Atallah. Early gdpr penalties: Analysis of implementation and fines through may 2020. *Journal of Information Policy*, 11:63–103, 2021.

[89] Ori Cohen. What is Parametric Insurance? Available: https://parametrixinsurance.com/what-is-parametric-insurance/, 2020. [Online; accessed 5-Feb-2023].

[90] GallagherRe. Cyber in the 2020s: A question of capacity. https://www.ajg.com/gallagherre/news-and-insights/2021/april/cyber-in-the-2020s/, 2021.

[91] Bank of England Prudential Regulation Authority. Supervisory statement | ss4/17: Cyber insurance underwriting risk. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2017/ss417, 2017. Accessed: 2023-02-8.

[92] Daniel W Woods and Andrew C. Simpson. Policy measures and cyber insurance: A framework. *Journal of Cyber Policy*, 2(2):209–226, 2017.

[93] Dirk Wrede, Tino Stegen, and Johann-Matthias Graf von der Schulenburg. Affirmative and silent cyber coverage in traditional insurance policies: Qualitative content analysis of selected insurance products from the german insurance market. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 45:657–689, 2020.

[94] Ian Newman, Ed Pocock, and Jemima Hall. CY–FI the future of cyber (re)insurance. https://www.ajg.com/gallagherre/news-and-insights/2022/february/future-of-cyber-reinsurance/, 2020.

[95] Martin Eling, Mauro Elvedi, and Greg Falco. The economic impact of extreme cyber risk scenarios. *North American Actuarial Journal*, pages 1–15, 2022.

[96] Tom Johansmeyer and Alex Mican. Cyber ils: How acute demand could drive a scalable retro market. *The Journal of Risk Management and Insurance*, 26(1):40–59, 2022.

[97] Tom Johansmeyer. The defence implications of increased cyber reinsurance concentrations. SOAS Blog https://study.soas.ac.uk/cyber-defence-implications-reinsurance/, 2022.

[98] Xiaoying Xie, Charles Lee, and Martin Eling. Cyber insurance offering and performance: An analysis of the us cyber insurance market. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 45:690–736, 2020.

[99] Luke Gallin. Silent cyber drives petya loss to $2.7 billion, says pcs. *Reinsurance News*, 2018. Accessed: 2023-02-8.

[100] Henry RK Skeoch and Christos Ioannidis. The barriers to sustainable risk transfer in the cyber-insurance market. *Journal of Cybersecurity*, 10(1):tyae003, 2024.

[101] Catrin Shi and Adam McNestrie. Munich Re takes hard line on narrower cyber war exclusions. *Insurance Insider*, 2023.

[102] The Insurer. Chubb cancels mammoth cyber QS as it mulls 2023 XoL. https://www.theinsurer.com/news/chubb-cancels-mammoth-cyber-qs-as-it-mulls-2023-xol/, 2023.

[103] Steve Evans. Operational re iv ltd., $217.25m op-risk cat bond issued, likely for credit suisse. https://www.artemis.bm/news/operational-re-iv-ltd-217-25m-op-risk-cat-bond-issued-likely-for-credit-suisse/, 2023. Accessed: 2023-02-8.

[104] Beazley. Beazley launches market's first cyber catastrophe bond. https://www.beazley.com/en-us/news/beazley-launches-markets-first-cyber-catastrophe-bond, 2023. Accessed: 2023-02-27.

[105] Evans, Steve. Swiss Re successfully prices market's first industry-loss cyber cat bond: Available: https://www.artemis.bm/news/swiss-re-prices-first-industry-loss-cyber-cat-bond/, 2023. [Online; accessed 11-Feb-2024].

[106] Steve Evans. Coalition launches $300m ferian re to provide third-party cyber risk capital. https://www.artemis.bm/news/coalition-launches-300m-ferian-re-to-provide-third-party-cyber-risk-capital/, 2022. Accessed: 2023-02-8.

[107] Steve Evans. Catastrophe bond market hits new record size of $38.2bn. https://www.artemis.bm/news/catastrophe-bond-market-hits-new-record-size-of-38-2bn/, 2023. Accessed: 2023-02-8.

[108] Nathan Bruschi. Maybe wall street has the solution to stopping cyber attacks. *Wired*, 2016. Accessed: 2023-02-8.

[109] Lerner, Matthew. Cyber insurers track privacy exposures: Available: https://www.businessinsurance.com/article/20230712/NEWS06/912358420/Cyber-insurers-track-privacy-exposures, 2023. [Online; accessed 19-Nov-2023].

[110] Eric Dal Moro. Towards an economic cyber loss index for parametric cover based on it security indicator: A preliminary analysis. *Risks*, 8(2):45, 2020.

[111] Tom Johansmeyer. Is the fear of cyberwar worse than cyberwar itself? https://www.lawfaremedia.org/article/is-the-fear-of-cyberwar-worse-than-cyberwar-itself, 2022.

[112] GuyCarpenter. Through the looking glass: Interrogating the key numbers behind today's cyber market. https://www.guycarp.com/insights/2023/05/through-the-looking-glass-interrogating-key-numbers-behind-todays-cyber-market.html, 2023. Accessed: 2023-06-06.

[113] Coalition. Active cyber risk modeling: a modern approach to cyber risk aggregation. https://info.coalitioninc.com/download-active-cyber-risk-model-2023-03-21.html, 2023. Accessed: 2023-06-06.

[114] Mathew Vermeer, Jonathan West, Alejandro Cuevas, Shuonan Niu, Nicolas Christin, Michel Van Eeten, Tobias Fiebig, Carlos Ganán, and Tyler Moore. Sok: A framework for asset discovery: Systematizing advances in network measurements for protecting organizations. In *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 440–456. IEEE, 2021.

[115] Serge Egelman, Marian Harbach, and Eyal Peer. Behavior ever follows intention? A validation of the security behavior intentions scale (SeBIS). In *Proc. of the Conf. on Human Factors in Computing Systems*, pages 5257–5261. ACM, 2016.

[116] Simson L Garfinkel. Digital forensics research: The next 10 years. *digital investigation*, 7:S64–S73, 2010.

[117] Lorenz Kustosch, Carlos Gañán, Mattis van't Schip, Michel van Eeten, and Simon Parkin. Measuring up to (reasonable) consumer expectations: Providing an empirical basis for holding iot manufacturers legally responsible. In *Proceedings of the 32nd USENIX Security Symposium*, 2023.

[118] Alex Clere. At-bay launches new admitted cyber insurance for small firms. *InsurTech*, 2023.

A CONTRACT EXTRACTS

Rurik's $5 million warranty [61] contains the following warranty:

> *"Rubrik shall only provide Payment to Customer if, at the time of the Ransomware Incident and throughout the Warranty Period:*
>
> (1) *Customer has maintained an active subscription for the Eligible Solution (Rubrik Enterprise Edition, Rubrik Cloud Vault (as applicable), and the CEM);*
> (2) *Customer had deployed the most recent version of the Eligible Solution software as further described in Section 4.3 with the latest security patch available prior to the applicable Ransomware Incident;*
> (3) *Customer had completed all Health Checks and implemented all Health Check recommendations in a timely manner;*
> (4) *The Event Date and Discovery Time of the Ransomware Incident occurred, was discovered by Customer, and reported to Rubrik during the Warranty Period, and in accordance with Section 5;*
> (5) *Customer has remained in compliance with its Customer Agreement, including without limitation any payment obligations;*
> (6) *Customer has fully cooperated with Rubrik, including without limitation by (i) implementing all remedial and security measures required by Rubrik including the Requirements, (ii) providing Rubrik with all documentation, permissions, and access to relevant systems and environments required to verify Customer is entitled to a Warranty Payment, and (iii) complying with the Reimbursement Request process set forth in Section 6;*
> (7) *Any systems to which the Customer seeks to restore Customer data successfully backed up by Rubrik are free of any malware, bugs, back-doors or other malicious code, and are otherwise secured; and*
> (8) *This Warranty is not restricted or prohibited by applicable law.*
>
> The contract includes further requirements, such as:
>
> *"**Data Security Best Practices.** Customer must follow the Rubrik security best practices as defined in the latest version of the Security Hardening Best Practices Guide, which can be found on the Rubrik support portal or provided upon request and includes without limitation the following:*
>
> *Data Health*
>
> - *Back-ups are successful and meet the SLA Policies*
> - *Retention lock is enabled for the Customer data in the SLA Policies*
>
> *User Access*
>
> - *Multi-factor authentication for all user accounts*
> - *SSH key-based with passphrase protected keys for CLI authentication*
> - *User roles are assigned with least privilege access*
>
> *Data Encryption*
>
> - *Data-at-rest and in-transit are always encrypted*
> - *Secure protocols for third-party systems*
>
> *Application Access*
>
> - *Create IP whitelisting that limits connections to Customer owned networks only*

- *SSL-certificate security for User Interface (UI) and APIs*

API Security

- *Secure service accounts*
- *Scoped API roles with least privilege"*