The supply of cyber risk insurance*

Martin Eling Anastasia Kartasheva Dingchen Ning

May 3, 2024

Abstract

Cyber risk economic losses are large and growing, yet the insurance market for cyber risk is tiny, amounting to 0.8% ($7.2 billion) of premiums in the US property-casualty insurance market in 2022. In this paper, we analyze the constraints that the insurance industry faces in providing larger capacity. We argue that cyber risk is special in that it combines (i) heavy-tailedness, (ii) uncertain loss distribution, and (iii) asymmetric information in underwriting. The combination of factors (i)-(iii) creates a tension between a need to raise substantial amounts of capital to finance heavy-tailed and uncertain risks and an expensive compensation demanded by investors due to information frictions. To circumvent asymmetric information costs, insurers can use internal capital. Hence, suppliers of cyber insurance are large insurance groups with a deep internal capital market. However, their capacity is constrained by the group's size. We document stylized facts about the US cyber risk insurance market. We then establish the causal inference that insurers primarily rely on the internal capital market to supply cyber risk insurance using an exogenous shock of the non-US affiliated reinsurance tax treatment in 2017. Finally, we test which of the three features (i)–(iii) of cyber risk contribute to the cost of external capital and confirm that all of them play a significant role.

Keywords: cyber risk insurance, large risks financing, internal capital market, reinsurance, information frictions.
JEL classification: G22, G32, L11.

*We thank Julia Holzapfel, Ralph Koijen, Andre Liebenberg, Alina Salzberger, Laura Veldkamp, Motohiro Yogo, and Marco Zanotti for insightful discussions, and the audiences at the ARIA, EGRIE, and DGF Annual Conferences, NY Fed - Columbia Workshop on Cyber Risks to Financial Stability, SFI Research Days, and the University of St.Gallen for helpful comments. All authors: Institute of Insurance Economics and School of Finance, University of St.Gallen, and Swiss Finance Institute.

1 Introduction

Cyber risk has become a major threat to individuals, businesses, and society. The US computer security software company, McAfee, estimated the costs of global cybercrime to be $1 trillion in 2020, more than 50% increase from the 2018 estimate of $600 billion (McAfee, 2020). Cybersecurity risk insurance (hereafter referred to as cyber insurance), which offers coverage against losses arising from cyber risk events, has drawn attention from various stakeholders as a means of protection against cyber risk economic exposures for firms and households. The cyber insurance market is emerging, as the premiums increased almost three times, from $1 billion to $7.2 billion in the US from 2015 to 2022. Yet, it is estimated that more than 90% of the cyber losses are not covered by insurers (Swiss Re Institute, 2022). Further, the size of the US cyber insurance market, which is the most developed market globally, is a tiny 0.8% fraction of its property and causality (P&C) insurance market in 2022 (NAIC, 2023).

In this paper, we explore how the underdevelopment of the cyber insurance market is related to supply-side factors. We point out that insurance of cyber risk is challenging due to the combination of its distinctive features: (i) heavy-tailedness, (ii) uncertain loss distribution, and (iii) information intensity. The possibility of extreme cyber losses that occur simultaneously during a short period of time limits the scope for cross-sectional diversification for the insurance industry (Ibragimov, Jaffee, and Walden, 2009). Similar to other large risks such as natural catastrophes or pandemics, underwriting cyber risk would require a significant amount of external capital (Jaffee and Russell, 1997; Froot, 2001; Gründl et al., 2021). However, the other two distinctive features of cyber risk are that it is highly uncertain and is encumbered with asymmetric information problems. Due to the information intensity of cyber risk, raising external capital can be expensive for insurance companies. Hence, the supply of cyber insurance relies heavily on the insurer's internal capital.

We argue that the availability of insurers' internal capital constrains the supply of cyber insurance. The insurers' internal capital market (ICM) operates within insurance groups by means of affiliated reinsurance (or internal reinsurance) among the group's subsidiaries.

The size of the ICM can be significant for larger insurance groups (Powell, Sommer, and Eckles, 2008; Niehaus, 2018). However, cyber insurance competes with other types of insurance offered by the insurer. The scarcity of internal capital curtails the amount of cyber insurance that the insurer is willing to provide.

To test these arguments empirically, we analyze the US cyber risk insurance market. We take advantage of a recent initiative by the National Association of Insurers Commissioners (NAIC), the US insurance industry regulator, that in 2015 started to collect data on cyber insurance supply by the US property and casualty (P&C) insurers. We first document the stylized facts about the cyber insurance market. We observe that large insurance groups dominate the cyber insurance market, with the top 5 and top 10 largest participants taking 33% and 52% of the market share in 2022, respectively. Further, despite the rapid growth of the cyber insurance market by 724% between 2015 and 2022, or 32.4% annually, the cyber insurers did not compromise profitability and did not increase the exposure to cyber risk. The data analysis reveals that insurers have been increasing the supply while also increasing the price, indicating the growing demand for cyber insurance.

The next stylized fact is that the ICM plays a significant role in cyber insurance supply. We find that, at the median level, cyber insurers reinsure at least 20% more than those underwriting other risks, that is, insurers retain less cyber risk compared to other risks. Furthermore, the majority of reinsurance for cyber insurers is obtained from affiliates of the same group, that is, the ICM. To highlight the importance of ICM for cyber risk, we estimate the correlation between the share of premiums in a given insurance line, including cyber, and the use of affiliated reinsurance. Our analysis reveals that cyber insurance is among the few lines showing a highly significant positive correlation with the utilization of affiliated reinsurance. This indicates that the use of affiliated reinsurance is a more inherent factor in the underwriting of cyber insurance compared to other types of risks.

To establish the causal relationship between access to the ICM and the supply of cyber risk insurance, we exploit the regulatory change in the tax treatment of non-US affiliated reinsurance, namely, the base erosion and anti-abuse tax (BEAT) reform of 2017. The affiliated subsidiaries providing reinsurance can be either US-based or non-US-based, located in other countries or off-shore territories such as Bermuda. The BEAT reform has significantly increased the costs of non-US affiliated reinsurance, and, as a consequence, it reduced its use by US insurers. Then we measure a cyber insurer's exposure to this reform by multiplying the cyber insurance premiums share in the total premiums and the share of gross premiums ceded (transferred) to non-US affiliated reinsurance before the reform. We then compare the performance of the highly exposed insurers (with exposure above the median) and of the less exposed insurers. The difference-in-difference estimates provide strong evidence that the supply of cyber insurance is affected by the availability of affiliated reinsurance. More specifically, insurers exposed to the BEAT costs shock experienced a drop in the growth rate of cyber premiums of 14% in 2018, 30% in 2019, and 22% in 2020 compared to the control group. The results are confirmed when we use the exposure as a continuous treatment.

To establish a benchmark for comparison, we examine the effect of the BEAT reform on other insurance lines. To support the hypothesis that the reliance of cyber risk insurance on ICM is distinctive from other insurance lines, it has to be the case that the BEAT reform has a less pronounced impact on other insurance lines. We construct a similar measure of exposure to BEAT reform for other lines as a placebo test and find no significant effects in the same period.

Next, we investigate which features of the cyber risk (i)–(iii) prevent insurers from transferring risk to the external capital market. We design empirical tests to analyze the relationship between the prevalence of features (i)–(iii) in the cyber insurer underwriting portfolio and the cost of external reinsurance. To determine the effects of (i) heavy-tailedness on external capital costs, we test whether the price of external (non-affiliated) reinsurance is positively related to the share of cyber insurance. To assess how (ii) uncertainty of cyber risk loss distribution affects the price of reinsurance, we use the data from mandatory reporting on the introduction and revision of insurance products. In particular, reinsurers may charge higher markups for insurers with less experience in cyber underwriting. We proxy the insurer's level of cyber knowledge and experience by the frequency of cyber product updates with the regulators and test whether the update frequency is negatively related to reinsurance prices. To test the role of (iii) information frictions, we build on the premise that reinsurers rely on the long-term relationship to limit moral hazard (Doherty and Smetters, 2005). We then develop the empirical tests to assess how the reinsurance price responds to experience rating, reinsurers' monitoring, and direct price control. We combine the factors related to features of the cyber risk in a single test and find that all features (i)-(iii) play a significant role in limiting an insurer's access to external capital to underwrite cyber risk.

This paper contributes to several strands of the literature. A few recent studies have analyzed the impact of cyber attacks on firms, indicating significant shareholder wealth loss and lower risk appetite (Kamiya et al., 2021), thus inducing strategic timing of the announcement after the attack to attenuate the negative market reaction (Foerderer and Schuetz, 2022). Florackis et al. (2023) show that cyber risk is priced in the cross-section of stock returns. Furthermore, cyberattacks have wider impacts through the network connection, such as the supply chain of the firm (Crosignani, Macchiavelli, and Silva, 2023) and the interconnected financial system (Eisenbach, Kovner, and Lee, 2022). To the best of our knowledge, our study is the first to analyze the ability of the insurance market to provide risk transfer for cyber risks.

Our analysis is also related to the corporate finance literature on ICM (Gertner, Scharfstein, and Stein, 1994; Diamond, 1994; Stein, 2002). The presence of the ICM is driven by the benefits of reducing information asymmetries and increasing the incentives for monitoring among subsidiaries compared to external capital. We contribute to this literature by focusing on a unique type of ICM for insurance companies — affiliated reinsurance, and providing evidence that insurers prefer affiliated reinsurance as the better-informed capital over non-affiliated reinsurance. We also contribute to the literature on the risk-sharing function of reinsurance (Borch, 1962) and its role in the insurer's capital structure (Garven and Lamm-Tennant, 2003; Plantin, 2006).

More broadly, our study adds to the recent literature analyzing the supply-side factors of the insurance market. Koijen and Yogo (2015), Koijen and Yogo (2022), and Ge (2022), among others, analyze how financial frictions affect the insurance market by impacting insurers' product prices and investment. We contribute to the literature by focusing on the role of internal capital in the supply of information-intensive risk coverage, that is, cyber risk.

The remainder of the paper proceeds as follows. The next section discusses the nature of the cyber risk. Section 3 describes the data on the cyber insurance market in the US. Section 4 summarizes the stylized facts about the cyber insurance market. Section 6 develops the hypotheses and tests to show the role of the ICM in cyber insurance supply. Section 7 presents the results on the relationship between the price of reinsurance and the features of cyber risk. Section 8 concludes the paper.

2 The Nature of Cyber Risk

Cyber risk embodies an extensive spectrum of potential threats posed to information and information systems. These risks include unauthorized data access resulting in breaches, malicious software attacks such as ransomware, and internal system errors that may compromise data integrity and security, among others. Cyber risk can be defined as an operational risk to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems, following Cebula and Young (2010).

In this section, we review the distinct features of cyber risk: heavy tails, loss distribution uncertainty, and information asymmetries. Although some of these features are typical for other insured risks, for example, natural catastrophes or product liability, the combination of these features and their intensity for cyber risk differentiates it from the other insured risks.

2.1 Heavy tails

Cyber risk exhibits heavy tails, and its loss distribution should be modeled by the family of heavy-tailed distributions. Several studies have analyzed the loss frequency and severity of the cyber risk by fitting existing statistical models or proposing new models using several datasets of cyber incidents: Privacy Rights Clearinghouse data (Eling and Loperfido, 2017; Farkas, Lopez, and Thomas, 2021), SAS operational risk data (Eling and Wirfs, 2019), and Advisen data (Aldasoro et al., 2022; Malavasi et al., 2022). In a recent study, Eling, Ibragimov, and Ning (2023) compare all three datasets and estimate the tail index of the cyber loss distribution, providing further evidence that cyber losses have heavy-tailedness. This property weakens the ability of insurers to underwrite cyber risk, as it can induce a non-diversification trap (Ibragimov, Jaffee, and Walden, 2009).

2.2 Uncertainty

Cyber risk is still largely unknown. One obstacle to understanding cyber risk is data. Although there are several available databases that were used to analyze cyber risk properties as cited above, the data are heavily biased toward data breaches. The reason is that data breaches are the only category that is compulsory to report under the US data breach notification law.[1] Other categories of cyber risk have less information, especially for non-listed firms that have no obligation to make cyber incidents public.[2]

An additional factor contributing to high uncertainty is that cyber risk is rapidly evolving over time and thus difficult to estimate. There are several studies exploring the time trends of cyber risk with divergent results, depending on how the data are sliced and the methodology (Woods and Böhme, 2021b). For the time period between 2005 and 2015, Edwards, Hofmeyr, and Forrest (2016) suggest the size and frequency of data breaches do not change significantly, while Romanosky (2016) provide evidence of the increasing intensity of data breaches. Using three different data sources, Eling, Ibragimov, and Ning (2023) show the difference might also be driven by report delay. They also find the trends of different cyber categories are heterogeneous, resulting in more challenges in managing cyber risk.

Lastly, Falco et al. (2019) emphasize the importance of cross-disciplinary collaboration,

[1] The notification law is implemented at the state level and there are variations related to the content and the implementation time, see https://www.ncsl.org/technology-and-communication/security-breach-notification-laws.

[2] Listed firms are required to disclose material cybersecurity incidents, but the rule was introduced only in 2023, https://www.sec.gov/news/press-release/2023-139.

as the scope of cyber risk encompasses computer science, economics, law, management, and political science. Taken together, the lack of data, the dynamic nature of cyber risk, and the cross-disciplinary collaboration hurdles increase the uncertainty of cyber risk. As a result, it increases the complexity and the costs of managing and underwriting cyber risk for insurance companies.

2.3 Information frictions

Information asymmetry issues pervade the underwriting of cyber risk. The first step of underwriting is to evaluate the risk level of the clients and negotiate the proper contract details if both parties (the insured and insurer) decide to sign the contract. Adverse selection is a typical issue in this stage, as the insured with higher risk tend to purchase insurance and get higher coverages. The insurers exploit various methods to screen the insured with high risks, such as security questionnaires and minimum requirements for IT infrastructure security and operational risk management. However, as cyber risk is an emerging risk and still not sufficiently understood, the questionnaires and minimum requirements vary significantly and thus provide different levels of information depending on the expertise of the cyber insurers (Romanosky et al., 2019).

After signing the contract, insurers also exert extensive efforts to contain the ex-post cost of cyber events (Baker and Shortland, 2023). For example, cyber insurance typically covers the cost of incident response services. As insurers are not experts in the management of information security, they allow the insured to use the service from third parties, such as law firms to contain litigation risk, forensics firms to investigate the cause of the loss, and IT security firms to restore the affected system. With different layers of parties involved, it is difficult for insurers to control the cost. Woods and Böhme (2021a) show that insurers gradually adopt measures such as controlling which firms are selected, negotiating prices ahead of time, and punishing low service quality. Therefore, the underwriting results of cyber insurance heavily depend on the information advantage and monitoring efforts of the insurer.

3 Data on Cybersecurity Insurance Market

3.1 Cybersecurity insurance coverage

According to NAIC (2022), cybersecurity insurance (cyber insurance) coverage is commercial insurance either through a single policy or multi-peril coverage part solely intended to help manage risks associated with exposures arising out of network intrusions and improper handling of electronic data. The covered risks may include direct losses to the policyholder (first party) or the liability claims of third parties that are caused by the insured cyber event (third party). Examples of the direct costs to the policyholder include business interruptions and extra expenses resulting from an unauthorized person preventing access to the Internet, the policyholder's website, or other parts of the policyholder's network; costs related to a data breach such as restoring data, forensic investigations, legal expenses, public relations, breach notification, and regulatory expenses; cyber extortion against the policyholder; and ransom payments. The third-party liability protection consists of coverage for the exposure arising out of theft or loss of client's or customer's digital assets, the introduction of malware and other malicious computer code to third parties, and liability and damages resulting from network failures, among others.

Cyber insurance policies offered in the US market are diverse in terms of coverage and exclusions, policy limits, and risk factors used for insurance pricing. Based on cyber insurance policies collected from state insurance regulators across New York, Pennsylvania, and California, Romanosky et al. (2019) use text thematic analysis to explore the variation of insurance contract terms. They find, for example, that while some clean-up costs such as public relations services are included in more than 60% of the policies, the direct costs of loss such as data loss are covered only by 20% of the policies. Furthermore, they uncover a large variation in terms of exclusions across policies. Similarly, using rate schedules filed in California, Woods, Moore, and Simpson (2021) analyze risk factor pricing in cyber insurance policies and find a diverse range of risk estimates by insurers.

3.2 Data construction

In 2015, recognizing a lack of actuarial data as a major hurdle for quantitative assessment and tailored regulation of the cyber insurance market, the NAIC developed a new mandatory cybersecurity and identity theft insurance coverage data supplement (NAIC, 2016). All insurers writing cyber insurance are required to report annually their claims, premiums, losses, expenses, and the number of in-force policies. We use these data for the period 2015–2022.

The supplement distinguishes between two features of insurance policies to define the market segments. The first feature is whether the policy applies to commercial or personal lines, that is, cybersecurity or identity theft insurance. Cybersecurity insurance is designed for businesses and offers protection against losses stemming from risks such as data breaches and business interruptions. Identity theft insurance is intended for individuals and provides compensation for losses resulting from theft of credit cards, social security numbers, or bank account numbers. The second feature is whether the policy is standalone or a part of package policies that include coverage for other non-cyber risks. Thus, the supplement identifies four market segments: cybersecurity package, cybersecurity standalone, identity theft package, and identity theft standalone.

According to the NAIC evaluation in 2023, the data reported in the supplement provide a partial view of the identity theft insurance market. The reason is that many entities in the identity theft market are not insurers but rather credit card companies and specialized identity theft protection service companies.[3] Recognizing the issue, NAIC's 2023 report indicates that the supplement does not provide meaningful data on the identity theft segment and recommends eliminating this reporting requirement from the cyber supplement.[4] For these reasons, we focus on the cybersecurity insurance data in our analysis.

We complement the cyber supplement information with the annual insurance regulatory filings obtained from S&P Capital IQ that contain balance sheet and income statement information, such as assets, premiums, losses, reinsurance, leverage, risk-based capital, etc.

[3] The reported identity theft segment has been relatively stagnant in 2015–2022 and had a significantly smaller size of $0.25 billion. The details can be found in Appendix A.

[4] See Blanks (E) Working Group request for comment 2023-05BWG Modified, https://content.naic.org/exposure-drafts

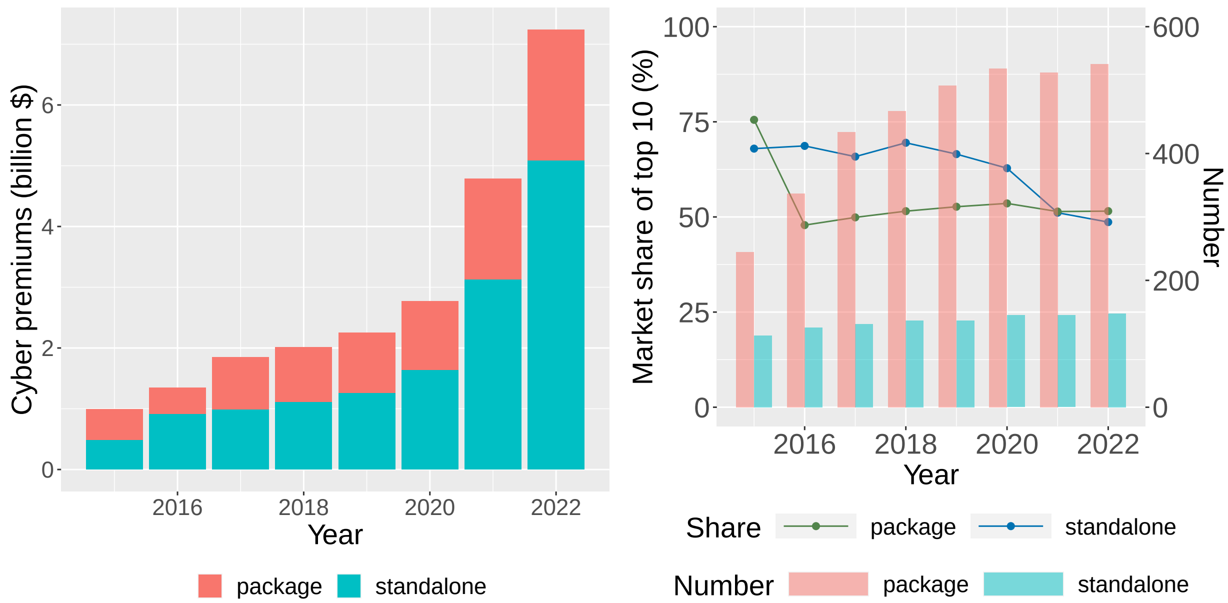

Figure 1: Cyber insurance market size

Note: The left figure compares the cyber premiums written for each market segment and the right figure presents the market share of the top 10 insurers and the number of participants in the cyber insurance market.

Where available, we obtain the data at the granularity of the business line of an insurance company. Typically, cyber package insurance is part of the commercial multiple peril line, and cyber standalone is part of the other liability line.[5] In addition, we use the insurer's financial strength ratings assigned by A.M. Best. We collect these data components for all property-casualty (P&C) insurance companies in the US for the period of 2015–2022 and merge them by NAIC company code to the cyber supplement data. The total number of firm-year observations for the sample of the US P&C insurers is 21,160, and for the sample of P&C insurers underwriting cyber insurance is 4,082.

3.3 Summary statistics

The left panel of Figure 1 depicts the premium volume of the cyber standalone insurance and cyber package insurance segments of the cyber insurance market. The cyber insurance market has grown significantly during the report period from $1 billion in 2015 to $7.24

[5]The NAIC line of business matrix distinguishes 35 lines of business; see https://content.naic.org/sites/default/files/ucaa-industry-lines-of-business-matrix.pdf.

billion in 2022. The growth was particularly pronounced for the standalone insurance segment whose size increased ten times during the reporting period. By 2022, standalone insurance accounted for 70% of the cyber insurance market. Figure 1, the right panel also shows an increasing number of insurers participating in the cyber insurance market, reaching a total of 606 firms in 2022.[6] However, the market is highly concentrated, with the market shares of the top ten insurers in standalone and package cyber insurance segments above 50% by 2022.

Table 1 reports summary statistics for the cyber insurance market. Although there are fewer standalone than package insurance policies, their average size, that is, the ratio of premiums to the number of policies, is significantly larger than the size of package policies. For example, 3.57 million package policies were issued in 2022, with a total volume of premiums of $2.15 billion. By comparison, only 0.34 million standalone policies were issued in the same year, but the premium volume was $5.09 billion. One reason is that standalone policies provide wider coverage and have higher prices compared to the package policies (Romanosky et al., 2019; Woods, Moore, and Simpson, 2021).

Standalone policies have a higher claim frequency of 4%-6% compared to the 0.01% claim frequency of package policies. Further, standalone policies' loss ratios, that is, the ratio of losses to premiums, are higher and more volatile than the loss ratios of package policies. Notably, the standalone segment seems to be impacted by the surge in cyber crime during the COVID-19 pandemic, as indicated by the 17% loss ratio increase from 2019 to 2020.

To evaluate the level of cyber insurance prices and compare it to prices charged for other insured risks, we calculate the inverse loss ratio, that is, the ratio of premiums to losses. In the insurance economics literature, the inverse loss ratio is commonly used as an indicator of insurance price (e.g., Harrington, 2004; Berry-Stölzle and Born, 2012). For one-year short-tail policies, the ratio equal to 1 corresponds to the actuarially fair price. Values of the ratio are usually above 1 signifying a positive price markup.

Table 2 compares the prices of the business lines where cybersecurity policies are booked and reported to the price of cyber lines calculated directly using the data from the supple-

[6] There are 83 insurers that provide both standalone and package cyber policies.

Table 1: Summary statistics for cyber insurance market

Year	Premiums (billion $)	Insurers	Insurance groups	Number of policies (million)	Claims frequency (%)	Cyber insurance market share (%)	Combined loss ratio (%)	Standard deviation of loss ratio
Cybersecurity package policy								
2015	0.51	245	95	0.86	0.00	0.09	2.33	8.89
2016	0.43	337	113	1.88	0.00	0.07	4.25	13.41
2017	0.86	434	141	2.47	0.01	0.14	23.95	126.19
2018	0.90	467	159	2.84	0.01	0.13	10.90	35.76
2019	0.99	507	176	3.15	0.01	0.14	11.47	38.50
2020	1.13	534	179	3.79	0.01	0.16	11.65	46.93
2021	1.66	528	193	3.51	0.01	0.21	13.48	48.25
2022	2.15	541	194	3.57	0.01	0.25	14.72	59.72
Cybersecurity Standalone Policy								
2015	0.49	113	43	0.07	0.00	0.08	34.75	89.11
2016	0.92	126	49	0.15	0.00	0.15	27.25	54.85
2017	0.99	131	55	0.10	3.95	0.16	43.26	153.48
2018	1.11	137	55	0.12	4.70	0.17	33.13	107.38
2019	1.26	137	58	0.16	6.15	0.18	27.00	37.96
2020	1.64	145	60	0.20	6.28	0.23	43.81	71.42
2021	3.13	145	62	0.26	5.20	0.39	55.45	99.04
2022	5.09	148	67	0.34	4.61	0.58	41.75	83.84

Note: This table presents summary statistics of key variables in the cyber insurance market by year. *Premiums* are calculated as the summation of cyber premiums of all insurers in the respective segment. The number of insurance groups includes independent insurance companies without group affiliation. *Claims frequency* is calculated as the total number of claims divided by the total number of policies in the respective segment. *Cyber insurance market share* is calculated as the cyber premiums of all insurers divided by the total premiums of all insurers. *Combined loss ratio* is the cyber loss incurred plus direct defense and cost containment expense (also known as allocated loss adjustment expense) divided by cyber premiums earned for each insurer and the mean value is reported in this table. The last two columns are calculated after winterizing the top and bottom 1%, as the extreme values significantly distort the statistics.

Table 2: Inverse loss ratio of cyber insurance compared to other lines

	Mean	Standard deviation	Min	1st quantile	Median	3rd quantile	Max	Sample size
Multi peril	1.02	0.33	0.05	0.86	1.00	1.16	2.22	3223
Other liability	1.23	0.67	0.05	0.85	1.09	1.45	3.98	5473
Cyber package	54.19	119.96	0.00	3.74	13.90	43.89	1095.21	1206
Cyber standalone	9.84	24.68	0.06	1.54	2.29	5.72	195.59	708

Note: This table presents the price of insurance, which is calculated as the inverse of the combined loss ratio for different insurance lines from 2015 to 2022. The data are censored at 95%, and all negative values are excluded. The values for *Multi peril* and *Other liability* are calculated after excluding all insurers that have cyber exposure during the sample period. The definition of lines of businesses can be found in Appendix B.

ment. Typically, the cyber package policies are categorized into the commercial multi-peril line and the cyber standalone policies are categorized into the other liability line. Compared to these insurance lines, the price of cyber lines has an extraordinarily higher price markup and much larger volatility. The mean value of the price is 54 times higher for the cyber package policy compared to a multi-peril policy and 8 times higher for the cyber standalone compared to the other liability line. Furthermore, the cyber insurance lines have striking differences across the quantiles.

Insurers can also utilize non-price methods to control their exposures to cyber risk in cyber insurance contracts. The reporting features of insurance contracts distinguish between occurrence and claims-made policies. Occurrence insurance policies cover insured events that occur within the effective dates of the policy regardless of when they are reported to the insurer. By contrast, claims-made policies cover insured events that are reported within the effective dates of the policy. Therefore, occurrence policies have a longer-term exposure than claims-made policies. In 2015–2022, cyber insurers diminished their risk by increasing the share of claims-made cyber policies. The share of standalone claims-made policies increased by 12.2% to 95.6%, and the share of package claims-made policies has increased by 11.8% to 48.8%. Furthermore, insurers mitigate their exposure by adjusting deductibles and coverage limits. NAIC (2021) reports that, due to the surge of cyber risk, the limits for cyber insurance policies dropped from $10 million to $5 million in 2020.

4 Stylized Facts about the Cyber Insurance Market

We now document several stylized facts about the cyber insurance market to illustrate how the unique features of the cyber risk summarized in Section 2 are reflected in the cyber insurance market structure. We start with the description of the market concentration and growth. We then evaluate the sources of capital that insurers use for underwriting cyber risk and detect a substantial reliance on the ICM which is in contrast to the capital structure of the other major insurance business lines. Lastly, we show that despite the rapid growth of the cyber insurance market, insurers selling cyber risk coverage maintain underwriting profits, suggesting that the leading cyber insurance providers succeed in limiting their exposure to cyber risk.

4.1 Market structure

Figure 1 and Table 1 report the number of insurers and insurance groups that provide cyber risk coverage. The number of insurers in the market steadily increased between 2015–2022, and it more than doubled for the package cyber insurance segment. For comparison, the number of P&C insurers increased on average by 1% during 2015–2022. Despite active entry, the market remained highly concentrated. As depicted in Figure 1, right panel, the top ten insurers accounted for more than 50% of the cyber standalone and package segments. Further, an average of 10 insurers exit the cyber insurance market every year. However, entry and exit are concentrated among small firms experimenting in a new market. The share of cyber insurance premiums in the aggregate P&C market also increased during 2015–2022 from 0.17% in 2015. However, the cyber insurance premiums still accounted for only 0.8% of the aggregate P&C insurance premiums, meaning that only a small share of cyber risk is insured.

Table 3 reports corporate characteristics of insurers underwriting cyber insurance (cyber insurers) and compares them to insurers not underwriting cyber risk (non-cyber insurers). Several features stand out. Cyber insurers tend to have larger market shares in the P&C insurance market and larger size. Although only 23% of P&C insurers underwrite cyber insurance, their market share in the P&C insurance market is 48%. In terms of assets, the median total assets of cyber insurers are $523 million for standalone policy writers and $296 million for package policy writers, compared to $51 million for non-cyber insurers. Cyber insurers have higher leverage ratios but similar A.M. Best ratings compared to non-cyber insurers.

More than 95% of cyber premiums are written by insurers that are members of insurance groups. At the group level, the exposure to cyber insurance liabilities of insurance groups underwriting cyber risk is insignificant. Even the top 5% cyber insurers by premiums have only 4.46% of their total group-level premiums in cyber standalone policies and 0.54% in cyber package policies.

Table 3: Corporate profile of cyber insurers in 2022

	All cyber	Cyber Standalone	Cyber Package	Non-cyber
Number of insurers	606	148	541	2039
Cyber premiums by groups (%)	97	98	95	0
Cyber share in the top 5% (%)	2.05	4.46	0.54	0
P&C market share (%)	48	16	42	52
Median value				
Total assets (million $)	311	523	296	51
Combined loss ratio (%)	94	85	95	87
Leverage (%)	58	63	57	48
Risk-based capital (%)	516	447	526	531
A.M. Best rating	A	A	A	A
Premium weighted average				
Total assets (billion $)	5	3	12	37
Combined loss ratio (%)	53	46	69	81
Leverage (%)	60	61	58	56
Risk-based capital (%)	1917	1883	1998	1630
A.M. Best rating	A+	A+	A+	A

Note: This table presents the key characteristics of cyber and non-cyber insurers. *Cyber premiums by groups (%)* is calculated as the percentage of cyber premiums written by insurers affiliated with insurance groups. *Cyber share in the top 5% (%)* is calculated as the share of cyber premiums in total group-level premiums for insurers ranked in the top 5% by cyber premiums. *P&C Market share* is calculated as total premiums written by insurers divided by the total premiums written in the P&C market. There are overlaps between insurers that underwrite cyber standalone policies and those insurers that underwrite cyber package policies, and thus the sum of their market shares is higher than the sum of all cyber insurers. *Total assets* is the total admitted assets in all lines reported. *Combined loss ratio (%)* is calculated as the total losses plus expenses divided by total premiums. *Leverage (%)* is calculated as total liabilities divided by total assets. *Risk-based capital (%)* is calculated as the ratio of total adjusted capital to risk-based capital requirement. **Median value** is calculated as the median level of the specified category. **Premium weighted average** is calculated as the sum of one statistic of the specified category weighted by cyber premiums for cyber insurers or total premiums for non-cyber insurers.

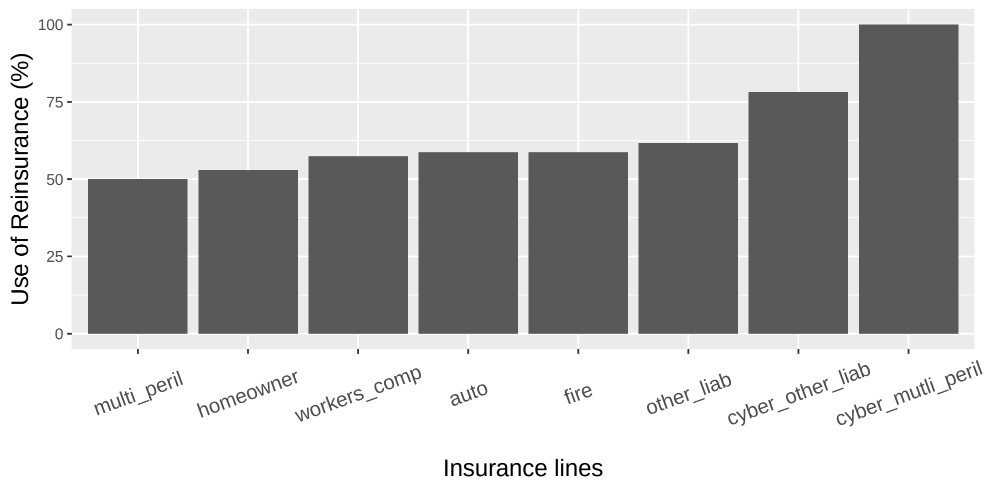

Figure 2: Use of reinsurance by insurance lines

Note: This figure presents the median use of reinsurance (% of total premiums) across different lines of business in 2022. *cyber_other_liab* and *cyber_mutli_peril* use the subsample of insurers with more than 50% cyber premiums in the corresponding lines.

4.2 Affiliated and non-affiliated reinsurance

Cyber insurers transfer more risk to reinsurers and retain less risk on their balance sheets compared to other insurers. Furthermore, the risk transfer and risk sharing of the cyber risk are more reliant on the ICM of the insurance group compared to other insured risks. In this section, we document evidence that supports these points by exploring the use of reinsurance by cyber and non-cyber insurers.

Reinsurance has unique institutional features, and some basic explanations are in order before we proceed with the analysis. Reinsurance is a risk-sharing mechanism that allows the primary insurers to transfer the underwriting risk to another insurer or reinsurer. Primary insurers may choose to limit the scale and scope of their operations to focus on core competencies such as marketing, underwriting, and loss control. However, the limited scale and scope also constrain the risk diversification in their liability portfolio. The economic rationale for reinsurance is that it allows for improved diversification by sharing risks with other insurers (Doherty, 1997).

Reinsurance treaties can occur between two independent insurers, an insurer and a specialized reinsurer, and insurers within the same insurance group. The last type is referred to as affiliated (or internal or intra-group) reinsurance, as it is a contract between affiliated subsidiaries of an insurance group. The former two types are referred to as non-affiliated (or third-party, or external) reinsurance. The share of affiliated and non-affiliated reinsurance in the US P&C insurance industry in 2022 is 77.2% and 22.8%, respectively. The dominant reliance on affiliated reinsurance is driven by the prevalence of insurance groups. More than 70% of all insurers and 90% of cyber insurers are affiliated with an insurance group in the US P&C insurance industry in 2022. Furthermore, affiliated reinsurance is the main form of ICM transaction used by insurance groups compared to other ICM transactions (Powell, Sommer, and Eckles, 2008; Cummins and Weiss, 2016;Niehaus, 2018).

Cyber insurers retain less risk and cede, that is, transfer, more risk to reinsurance compared to other insurers. Figure 2 depicts the use of reinsurance across different lines of business, including cyber. It shows that insurers focused on cyber insurance lines transfer a significantly higher share of their premiums to reinsurers. For example, in the multi-peril line, non-cyber insurers cede 50% premiums to reinsurers at the median level. By contrast, insurers that have more than 50% cyber premiums in this line transfer almost all premiums to reinsurance. Across non-cyber lines, the use of reinsurance ranges between 50% and 60%, while in lines with more than 50% cyber exposure, the reliance on reinsurance exceeds 75%.

Table 4 summarizes the reinsurance activity of cyber and non-cyber insurers. Although cyber insurance is only a small part of the insurers' business, the difference in utilization of reinsurance between cyber insurers and non-cyber insurers is apparent. At the median level, of all premiums written in 2022, cyber insurers retain 30% and cede 50% to their affiliates, while non-cyber insurers retain around 50% and cede a negligible amount of premiums within their groups. If we consider the reinsurance activities of insurers weighted by their premiums, the role of ICM for non-cyber insurers increases significantly. The reason is that the large non-cyber insurers that dominate the market transfer a substantial amount of premiums to their affiliates. However, even in comparison with large non-cyber insurers, cyber insurers still have a 15% lower retention ratio and 6% higher affiliated reinsurance, suggesting that cyber insurers rely heavily on the use of affiliated reinsurance.

To further explore the role of affiliated reinsurance activities for underwriting cyber risk,

Table 4: Comparison of reinsurance activities in 2022

	All cyber	Cyber standalone	Cyber package	Non-cyber
Number of firms	606	148	541	2039
Median value				
Retention ratio (%)	31.75	20.95	32.18	51.19
US affiliated reinsurance (%)	49.59	35.82	51.95	0.00
Foreign affiliated reinsurance (%)	0.00	0.00	0.00	0.00
Non-affiliated reinsurance (%)	3.58	11.93	3.05	2.38
Premium weighted average				
Retention ratio (%)	25.42	23.60	29.75	40.55
US affiliated reinsurance (%)	53.43	54.23	51.52	47.15
Foreign affiliated reinsurance (%)	1.49	0.88	2.95	1.38
Non-affiliated reinsurance (%)	18.53	19.69	15.78	9.39

Note: This table presents the comparison of reinsurance activities of cyber insurers and non-cyber insurers in 2022. *Retention ratio (%)* is the ratio of premiums retained by the insurer to the total premiums. *US affiliated reinsurance (%)* is the ratio of premiums ceded to US affiliates to the total premiums. *Foreign affiliated reinsurance (%)* is the ratio of premiums ceded to US affiliates to the total premiums. *Non-affiliated reinsurance (%)* is the ratio of premiums ceded to external reinsurers to the total premiums. **Median value** is calculated as the median level of the specified category. **Premium weighted average** is calculated as the sum of one statistic of the specified category weighted by cyber premiums for cyber insurers or total premiums for non-cyber insurers.

we calculate the correlation between the share of premiums ceded to affiliated reinsurance and the share of premiums written across various lines of business of an insurer. We estimate the following ordinary least squares regression,

$$Affiliated\ Reinsuarnce_{it} = \beta_0 + \beta_1 cyber_{it} + \sum_j \beta_j line_{ijt} + X'_{it}\lambda + \epsilon_{it}, \quad (1)$$

where the dependent variable $Affiliated\ Reinsuarnce_{it}$ is the percentage of gross premiums of the insurer ceded to its affiliates. The variable $cyber_{it}$ is defined as the percentage of cyber premiums in gross premiums written by the insurer. The variable $line_{ijt}$ is defined as the percentage of premiums of the line j in gross premiums written by the insurer, and this includes all lines of businesses for P&C insurers.[7] Vector X_{it} includes control variables such as the size and leverage of the insurer, and others. Our main coefficient of interest

[7]More details on these lines can be found in Appendix B.

is β_1. If β_1 is positive and significant, it means that the underwriting of cyber insurance is positively correlated with the usage of affiliated reinsurance. Furthermore, if the other coefficients β_j are insignificant or negative, it would suggest that affiliated reinsurance has a unique role in cyber insurance supply.

To exclude the potential impact of the BEAT reform (which will be explained in the following section) in 2018 on our estimation, we consider the sample period from 2015 to 2017. In addition, our sample is restricted to insurers with premiums above the first quartile ($3 million) and insurers that are affiliated with a group.

Table 5 presents the estimates of Equation 1. We find that a higher percentage of cyber premiums is positively correlated with more intensive use of affiliated reinsurance. Using the estimates in column (3), a 1% increase in the share of cyber premiums is associated with a 1.39% increase in gross premiums ceded to affiliates. Remarkably, the effect is not present for other insurance lines when compared to the reference group (the commercial multi-peril line). For most insurance lines, the share of premiums in the line is either insignificant or negatively correlated with the share of affiliated reinsurance.

Lastly, a typical form of affiliated reinsurance is intercompany pooling agreements, under which all of the pooled business is ceded to the lead entity and then retroceded back to the pool participants in accordance with their stipulated shares (NAIC, 1998). For example, American Insurance Group, one of the largest insurance groups in the US, utilizes such an agreement, mandating all its P&C subsidiaries to cede 100% of its policyholder assets and liabilities to the lead insurer, National Union Fire Insurance Company. Subsequently, each member assumes its share of the pooled assets and liabilities as per the pre-specified agreement. The presence of these agreements enables insurance groups to diversify underwriting risks and ensure the solvency of nascent or smaller subsidiaries.

Due to the strong interconnection among the subsidiaries under the pooling agreement, their performance and financial strength are related. Hence, the rating agency A.M. Best identifies the companies that are members of the same pooling agreement as one rating unit and assigns the same rating to these insurance companies. Because of this, we will use measures at the rating-unit level when reinsurance decisions are involved in the analysis.

Table 5: Affiliated reinsurance and different lines of business

Dependent variable	Use of affiliated reinsurance (%)		
Model	(1)	(2)	(3)
Cyber	1.728**	1.346**	1.391**
	(0.7161)	(0.5595)	(0.5781)
Homeowner	-0.1942***	-0.1469***	-0.1474***
	(0.0648)	(0.0490)	(0.0492)
Accident & health	-0.7094***	-0.4461***	-0.4295***
	(0.1170)	(0.1200)	(0.1192)
Fire	-0.2417***	-0.1460**	-0.1425**
	(0.0804)	(0.0645)	(0.0644)
Auto damage	-0.0367	0.0184	0.0260
	(0.0572)	(0.0414)	(0.0417)
Financial	-0.5869***	-0.3127***	-0.3132***
	(0.0603)	(0.1015)	(0.0961)
Marine	-0.1531	-0.0048	0.0136
	(0.1435)	(0.1221)	(0.1230)
Medical	-0.0587	0.0630	0.0471
	(0.0900)	(0.0775)	(0.0783)
Workers	-0.1013	0.0189	0.0130
	(0.0645)	(0.0502)	(0.0506)
Other liability	-0.2331***	-0.0753	-0.0731
	(0.0690)	(0.0547)	(0.0548)
Auto liability	-0.3049***	-0.1516**	-0.1557**
	(0.0950)	(0.0760)	(0.0756)
Aircraft	-0.3851*	-0.2325	-0.2293
	(0.2270)	(0.2239)	(0.2196)
Fidelity	-0.4127***	-0.3498***	-0.3520***
	(0.1012)	(0.0876)	(0.0885)
Other	-0.2924***	-0.2692***	-0.2657**
	(0.1091)	(0.1032)	(0.1038)
Year FE	N	N	Y
Control	N	Y	Y
Observations	3,738	3,738	3,738
R^2	0.06417	0.33659	0.33960

Note: This table presents estimates of the relationship between the use of affiliated reinsurance and the percentage of different lines of business. The dependent variable is the continuous value, defined as the percentage of gross premiums written ceded to affiliates. The reference line is the commercial multi-peril line, which means the coefficients of different lines are interpreted compared to this line. Clustered standard errors at the insurer level are reported in parentheses. ***, **, and * denote the statistical significance at the 1%, 5%, and 10% level, respectively.

Table 6: Loss growth and premiums/claims growth

Dependent Variables:	Change in loss ratio			Change in loss ratio		
Model:	(1)	(2)	(3)	(4)	(5)	(6)
Change in premiums	-0.3472**	-0.3896***	-0.5899***			
	(0.1393)	(0.1002)	(0.1649)			
Change in claim count				0.2566***	0.2535***	0.2559***
				(0.0743)	(0.0696)	(0.0890)
Controls	No	Yes	Yes	No	Yes	Yes
Firm	No	No	Yes	No	No	Yes
Year	No	Yes	Yes	No	Yes	Yes
Observations	1,011	1,011	1,011	898	898	898
R^2	0.01362	0.02994	0.38544	0.01589	0.03435	0.36665

Note: This table presents the results for the relationship between loss ratio changes and premiums changes for cyber standalone and package policies. The sample is restricted to the observations that have reasonable growth ratios between 0 and 1000%. Signif. Codes: ***: 0.01, **: 0.05, *: 0.1

4.3 Premium growth and risk

The left panel of Figure 1 depicts a fast growth of cyber insurance premiums. The rapid growth of the cyber insurance market can be driven by inadequate pricing or reserving. Conversely, premium growth could be the result of the increasing insurance price per exposure. Following the analysis of Barth and Eckles (2009), we explore how the cyber insurance premium growth is related to cyber insurance underwriting risk.

Barth and Eckles (2009) develop a simple test to assess whether premium growth indicates more risk to estimate whether the premium growth and the claim count growth are positively related to the growth of the loss ratio. The test builds on the premise that premium volume is the product of the average rate and the number of exposures. Thus, premium growth can be achieved through either selling more policies and increasing the number of exposures or increasing the average price per exposure. An increase in the number of exposures can also require cutting the average rate per exposure and thus increase the risk. If the premium growth is achieved by reducing the price of exposures or adding more risky exposures, it will be positively correlated with the growth of the loss ratios. Further, if the exposure growth is obtained due to increased risk, the growth of claims count will be positively correlated with the growth of loss ratios.

To assess the implication of the rapid market growth for risk and profitability of insurers, we estimate the following two regressions,

$$ln(\frac{LR_{i,t}}{LR_{i,t-1}}) = \beta_i + \beta ln(\frac{P_{i,t}}{P_{i,t-1}}) + \epsilon_{i,t}, \tag{2}$$

$$ln(\frac{LR_{i,t}}{LR_{i,t-1}}) = \phi_i + \phi ln(\frac{C_{i,t}}{C_{i,t-1}}) + \epsilon_{i,t}, \tag{3}$$

where LR is the loss ratio, P is the premium, and C is claim count, i stands for insurer, and t refers to the year. If the growth of the premiums derives from increasing the risk, the estimated coefficients β and ϕ will be positive and significant.

Tables 6 report the results of the estimation of equations 2 and 3 for the combination of standalone and package cyber insurance market segments. In column (1)-(3), the results show the growth of premiums leads to lower loss ratios, which suggests that insurers succeed in containing their exposure to cyber risk despite the market growth. In column (4)-(6), the growth of claim count is positively correlated with the growth of loss ratios, indicating the increased claims lead to higher than average losses.

Although we cannot observe cyber insurance prices charged by insurers to firms, an increasing willingness to pay for cyber insurance policies by firms is a plausible explanation for interpreting the estimation results. NAIC (2021) cites several market surveys and industry reports that indicate cyber insurance price growth of 10-30% in 2020, possibly driven by increasing corporate demand for cyber insurance.

5 A Model of Risk Financing

We build a model that explains how the pecking order of financing sources depends on the insurance liability portfolio characteristics. We model financing choices between internal capital market, external reinsurance, outside investors. As in seminal papers on internal capital market by Gertner et al. (1994) and Stein (1997), the distinguishing characteristics of the funding sources are information asymmetry, allocation of control rights and asset redeployment, and managerial incentives. Gertner et al. (1994) and Stein (1997) emphasize that in an internal capital market, individual project managers do not raise funds directly from outside investors. Rather, the corporate headquarters acts as an intermediary between the project managers and outside investors. The headquaters raises funds from outside investors and possesses the control rights to distribute the funds to individual projects. Furthermore, headquaters has monitoring skills that enable it to acquire information about the projects ex ante prospects. We adopt these ideas to the insurance context. In addition, we extend the model by introducing prudential capital requirements which is a distinctive feature of operation of the insurance companies that are subject to solvency requirements.

5.1 Assumptions

Insurance company's liability portfolios. An insurance company consists of the headquarters and two divisions, safe and risky. It operates in two dates. At date $t = 0$, each division collects insurance premiums. At $t = 1$, it pays the indemnity to policyholders according to the realized losses. The safe division collects 2 units of premiums at $t = 0$ and realizes a loss of $2 - 2s$ at $t = 1$. Profits $2s > 0$ reflect the underwriting and investment profits of the division. A commodity-like insurance with many small and diversifiable losses such as private auto physical damage insurance is an example of a business line with such properties.

Risky division is the prototype of a division underwriting cyber risks. Risky division can choose different sizes of the liability portfolio, by collecting premiums in the amount $i \in \{0, 1, 2\}$. The division loss distribution is uncertain and depends on the portfolio size and the state of the world (Figure 3).

The loss of an insurance portfolio of size 1 is either $1 - y_H$ with probability μ or $1 + y_L$ with probability $1 - \mu$, with $0 < \mu < 1$. Then the net present value (NPV) of the risky division with liability portfolio of size 1 is $y_1 = \mu y_H - (1 - \mu) y_L$. We assume that $y_1 > 0$.

The distribution of losses of a larger portfolio of size 2 depends on the state of the world $\omega \in \{B, G\}$. The ex-ante probability of state G and state B occurring is p and $1 - p$, respectively, with $0 < p < 1$. In state B (”bad” state), a portfolio of size 2 of premiums realizes a loss of either $2 - 2y_H$ with probability $\mu - \lambda$ or $2 + 2y_L$ with probability

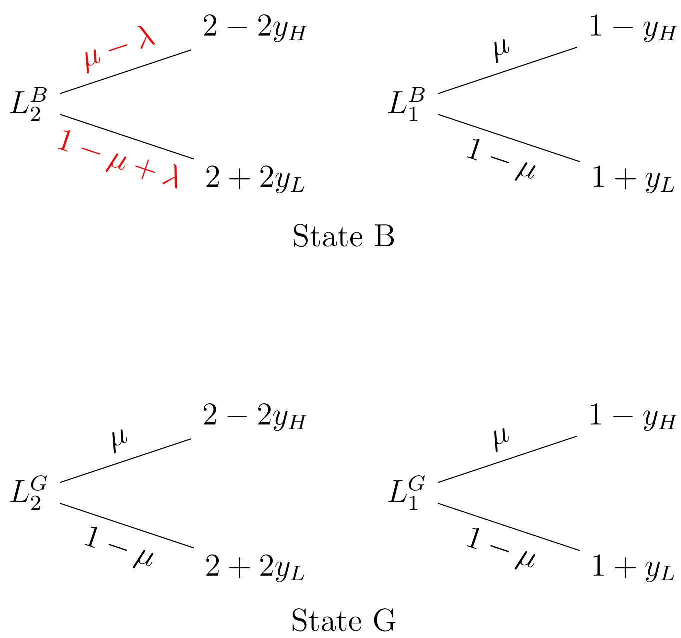

Figure 3: Loss distribution

$1-\mu+\lambda$, with $0<\mu-\lambda<1$. That is, in state B, a larger portfolio with 2 units of premiums is more likely to incur a large loss than a smaller portfolio with 1 units of premiums. The NPV of the risky division with liability portfolio of size 2 in state B is $y_2^B = 2(\mu y_H - (1-\mu)y_L) - 2\lambda(y_H + y_L)$. We assume that $y_2^B > 0$.

When the state of the world is G ("good" state), a portfolio of 2 units of premiums realizes a loss of either $2-2y_H$ with probability μ or a loss $2+2y_L$ with probability $1-\mu$. In this state, the NPV of the risky division of size 2 is $y_2^G = 2y_1$.

Assumption 1. *The efficient size of the division depends on the state ω.* The efficient size of the risky division is 2 in state G and 1 in state B, $y_2^B < y_1$. In terms of the model parameters, we assume that $\mu < \lambda < \frac{1}{2}\mu - \frac{1}{2}\frac{y_L}{y_H+y_L}$.

Prudential regulatory requirements and capital sources. The regulatory requirement is that an insurance division must be solvent for all loss realizations. We normalize the equity of a risky division to zero. It implies that the insurer needs to obtain contingent capital which is paid in states where the realized losses exceed insurers' premiums/reserves. The minimum required amount of contingent capital is $R_i = iy_L$ for the portfolio of size $i=\{1,2\}$.

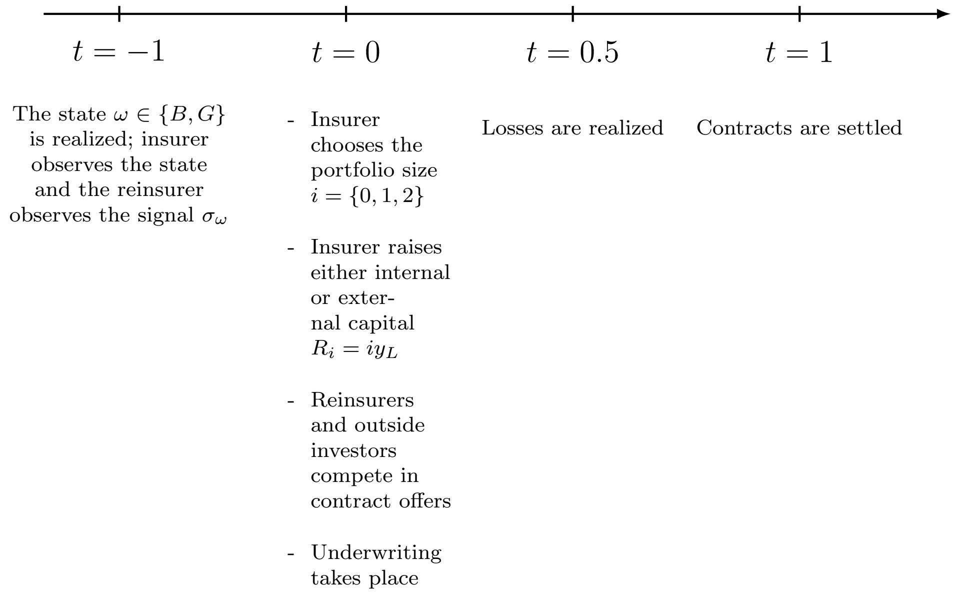

Figure 4: Timing

There are three potential sources for raising capital. Under internal capital market financing intermediated by the headquarters, the risky division obtains affiliated reinsurance from the safe division. Under external reinsurance, the insurer signs a reinsurance treaty with an unaffiliated reinsurer. Under capital market financing, the capital is obtained from outside investors. The insurer can combine any of these sources of capital. These capital sources differ in terms of the information available to capital providers, the ability of capital providers to direct the portfolio choice of the risky insurance division, and the agency costs.

Information structure. The distribution of states $P(G) = p$ and $P(B) = 1 - p$ is common knowledge. The manager of the risky division and the headquarters observe the state ω, but the outside investors do not. A reinsurer receives an informative signal σ_ω about the state of the world ω, with symmetric signal precision

$$q = P(G|\sigma_G) = P(B|\sigma_B) \geq \frac{1}{2}. \tag{4}$$

When $q = 1$, the reinsurer is perfectly informed about the state ω. When $q = \frac{1}{2}$, the reinsurer has no information advantage compared to the outside investors.

Timing. The timing of the model is depicted on Figure 4. Prior to any contracting, the state $\omega \in \{B, G\}$ is realized. An insurer observes the state ω and the reinsurer observes the signal σ_ω. At date $t = 0$, the division manager chooses the portfolio size of the risky division, i, and raises either internal or external capital $R_i = iy_L$ from reinsurers or outside investors who compete in contract offers. Then the underwriting takes place. In the interim date, the losses are realized. At date $t = 1$, all contracts are settled.

Payoffs. Our focus is the analysis of the role that the internal capital market plays in providing capital for underwriting insurance portfolios with different risk characteristics. While internal capital market alleviates the information asymmetries faced by the outsize investors and the headquarters are capable to direct funds to individual projects, delegation of decisions to headquarters also creates agency costs. Also, the amount of internal capital that the headquarters can provide to the risky division is constrained by the size of insurer's internal capital market. To reflect these features, we make the following assumptions on the payoffs.

Assumption 2. *Inclination towards over investment.* Divisions' and headquarters' managers tend to overstate their investment prospects.

Assumption 3. *Effort dilution.* Headquarters has residual control rights but reduces managers' ex-ante incentives to put forth effort.

Assumption 4. *Competitive financial market.* Reinsurers and investors compete in contract offers and earn zero profits.

Assumption 1 builds on the ideas developed by Gertner, Scharfstein and Stein 1994 and Stein 1997. We assume that division managers derive private benefits equal to the fraction $\delta \in (0, 1)$ of the cash flow. no revelation schemes are used

5.2 Division-level financing and credit rationing

We start by analyzing the benchmark case where each division raises contingent capital directly from reinsurers or outside investors. As there is no revelation schemes which can be used by the outside investors to make financing contingent on the state of the world, the investors can provide capital to support underwriting of either 1 or 2 units of premiums. Furthermore, we assume that the reinsurer does not have any information advantage compared to the outside investors.

In case of a small liability portfolio of size 1, the NPV of the risky division is y_1 regardless of the state of the world. In this case, the outside investors provide contingent capital in the amount y_L and charge the premium $P_1 = (1 - \mu)y_L$.

6 The Role of Internal Capital Market in the Supply of Cyber Insurance

We have documented evidence that the cyber risk insurance market is dominated by large insurance groups and that cyber insurers rely extensively on the ICM in the form of affiliated reinsurance to finance cyber risk underwriting. In this section, we aim to establish a causal relationship between the availability of affiliated reinsurance and the supply of cyber insurance. We first develop a theoretical model that explains the different roles of affiliated and non-affiliated reinsurance and build on it to formulate the hypotheses. We then describe the institutional details of the BEAT reform that we use as an external shock to the cost of affiliated reinsurance to enable us to establish a causal relationship. Next, we formulate our empirical tests and report the estimation results.

6.1 Theoretical background and hypotheses

[review to shorten and focus Hypothesis will need to be integrated in the model] The demand for reinsurance arises as it enables optimal risk sharing among risk-averse insurers (Borch, 1962). The risk aversion of insurers is driven by the sensitivity of policyholders to insurers' default risk (Doherty and Schlesinger, 1990), cost of financial distress, agency costs of external capital, and capital market frictions to hedge insurance-specific risks (Froot, Scharfstein, and Stein, 1993; Froot and Stein, 1998; Froot, 2007). Reinsurance is used to manage these risks and agency costs and thus plays a dual role of risk management and financing tool (Garven and Lamm-Tennant, 2003; Plantin, 2006). However, the empirical evidence indicates that external reinsurance, that is, the reinsurance purchased from unaffiliated reinsurers, is significantly lower than the optimal level, possibly because its price is distorted upwards by capital market frictions and reinsurers' market power (Froot, 2001; Froot and O'Connell, 2008).

To circumvent the excessive cost of external reinsurance and overcome agency problems, insurers often rely on the ICM where there is more scope for monitoring the risk-taking of the subsidiaries and the information asymmetries are less severe, resulting in the lower cost of internal capital compared to the external capital (Diamond, 1994; Stein, 2002). The previous empirical literature has documented that insurance groups rely extensively on ICM in the form of affiliated reinsurance (Powell and Sommer, 2007; Powell, Sommer, and Eckles, 2008; Fier, McCullough, and Carson, 2013; Niehaus, 2018). In addition, the group structure can isolate either the group from a risky subsidiary, or a subsidiary from the rest of the group, due to the limited liability of the subsidiaries and the headquarters. The group structure then affects the group's risk-bearing capacity and, therefore, has an impact on the costs of financial distress and the cost of debt (Luciano and Nicodano, 2014; Nicodano and Regis, 2019).

The information intensity of cyber risk discussed in Section 2 implies that the difference in the cost of external and internal capital can be pronounced. Yet, the cyber risk loss distribution features may require more capital per unit of exposure for underwriting cyber risk compared to other insured risks. The stylized facts about the US insurance market also indicate that insurers underwriting cyber risk rely more heavily on affiliated reinsurance. We further hypothesize that when the availability of affiliated reinsurance is reduced or its cost is increased, the supply of cyber insurance will be reduced, as the insurers rely heavily on affiliated reinsurance to diversify their cyber portfolio. We also hypothesize that the effect of a shock will be less pronounced for other types of insurance. Hence, we formulate the following two hypotheses:

- Hypothesis 1: The supply of cyber insurance decreases following the shock to the cost of affiliated reinsurance.

- Hypothesis 2: The supply of other types of insurance is less affected by the shock to the cost of affiliated reinsurance.

In the next section, we propose the empirical methodology to test these hypotheses and report the results.

6.2 The BEAT reform

To establish a causal inference, we assess the impact of the external shock that increased the price of affiliated reinsurance transferred by insurance groups to their subsidiaries outside the US, primarily in Bermuda which is traditionally a large reinsurance market. In 2017, the Tax Cuts and Jobs Act introduced the Base Erosion and Anti-abuse Tax (BEAT) to more effectively limit profit shifting and curb base erosion. BEAT designates a minimum tax of 10% that applies to certain multinational companies that make "base erosion payments" to foreign-related parties. To be subject to the BEAT, a corporate taxpayer must satisfy the following criteria:

- Have average annual gross receipts of at least $500 million for the prior three tax years.
- Have a base erosion percentage for the taxable year of 3% or more, 2% for some industries. The threshold is generally calculated by dividing the aggregate amount of the taxpayer's "base erosion tax benefits," or deductions attributable to "base erosion payments," by the total amount of the taxpayer's deductions for the year.
- Not be a regulated investment company, real estate investment trust, or S corporation.[8]

According to the tax regulation, a taxpayer who is a member of an aggregate group determines their status as an applicable taxpayer by reference to the gross receipts and the base erosion percentage of the aggregate group. This means that small subsidiaries of a large group are also affected by this reform.

For insurance companies, there are two types of cross-country affiliated transactions that are unique compared to other multinational companies: reinsurance transferred to an

[8]The S corporation is a business structure that is permitted under the tax code to pass its taxable income, credits, deductions, and losses directly to its shareholders.

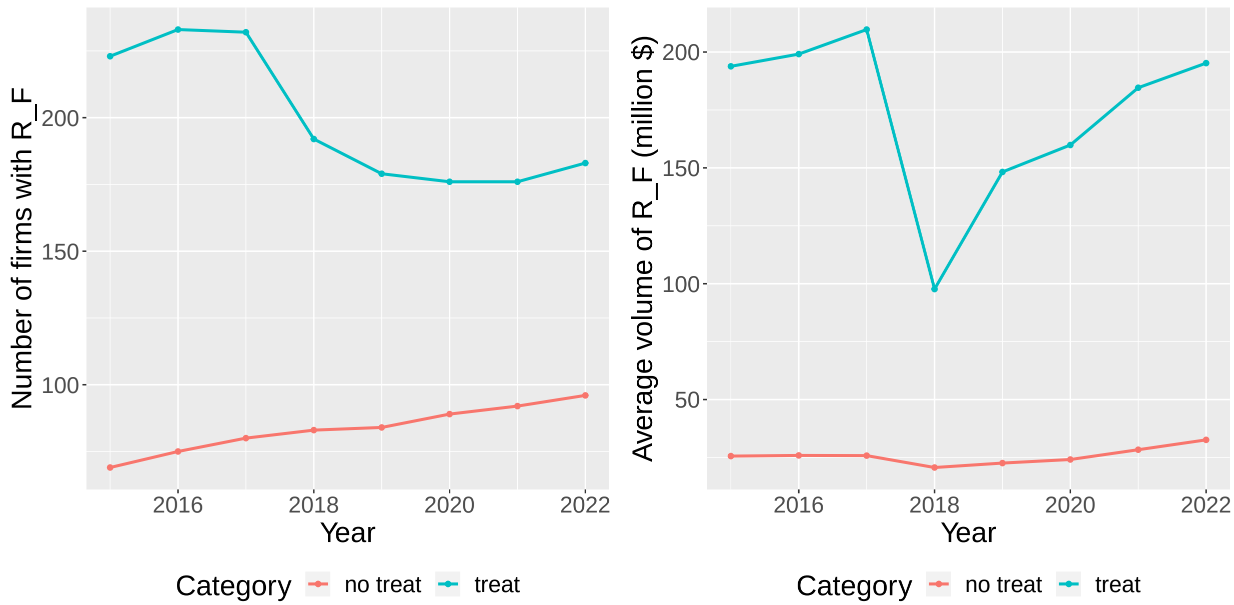

Figure 5: The impact of the BEAT on the use of non-US affiliated reinsurance

Note: This figure presents the non-US affiliated reinsurance (R_F) usage of all insurers in the market. The treatment group is the insurers with gross premiums higher than $500 million, and the non-treatment group is the insurers with gross premiums lower than this threshold. The percentage is calculated as the number of firms using non-US affiliated reinsurance divided by the number of firms in the group. The average volume is calculated as the mean value of non-US affiliated reinsurance premiums in the respective group.

affiliated foreign insurer, and claims payments made to an affiliated foreign insurer. The latter is exempted from the BEAT tax liability but the former is not. Therefore, this tax reform impacts the use of non-US affiliated reinsurance significantly.

To further understand the impact of the BEAT, we classify insurers into two groups based on their gross premiums written in the past three years. We rely on the first criterion above to define the treatment group, as we do not have enough information to calculate the base erosion percentage and the third criterion is not relevant for insurance companies. As shown in Figure 5, the reform affects the treatment group significantly, as both the number of insurers using non-US affiliated reinsurance (R_F) (extensive margin) and the average volume (intensive margin) decrease.

6.3 The impact of reinsurance cost shock on cyber insurance supply

We next examine Hypothesis 1 that the supply of cyber insurance decreases following the shock to the availability of affiliated reinsurance using the exogenous shock of the BEAT reform. To test it, we specify the following difference-in-difference (DiD) model:

$$Y_{it} = \alpha + \beta_1 D_i + \beta_2 Post_t + \delta(D \times Post)_{it} + X'_{it}\lambda + \tau_t + \sigma_i + \epsilon_{it} \quad (5)$$

where the subscripts i and t represent the firm and the year. The dependent variable, Y_{it}, is the outcome variable that measures the supply of cyber insurance. We consider two outcome variables, the growth rate of cyber premiums of the insurer compared to the previous year, and the growth rate in cyber insurance market share of the insurer i at time t. The latter also takes into account the competition in the market. The choice of outcome variables is discussed in Appendix C.

To check the parallel assumption for DID analysis, we adjust the standard DiD model by including periods before reform. We consider a binary treatment measure, $D_i = 1$ if the firm i is above the threshold of \$500 million gross premiums and $D_i = 0$ otherwise. Figure 6 shows the results of event study and there is no significant difference before the BEAT reform between the treatment and control firms, providing evidence that parallel assumptions hold. The effects on the growth of cyber premiums and market shares are significantly negative after the reform.

However, as the insurers affected by the BEAT reform are those with more than \$500 million in gross premiums, insurers that fall below this threshold may not be the suitable control group, since there are various factors linked to the firm size that affect the validity of comparison. To address this concern, we also consider the continuous measure of D_i that exploits the variation of insurers' exposure to the BEAT reform within the treatment group. The exposure is related to two factors, the size of cyber premiums and the share of non-US affiliated reinsurance in gross premiums. As reinsurance is reported on the level of an insurer, which can underwrite different lines of insurance, we allocate the reinsurance

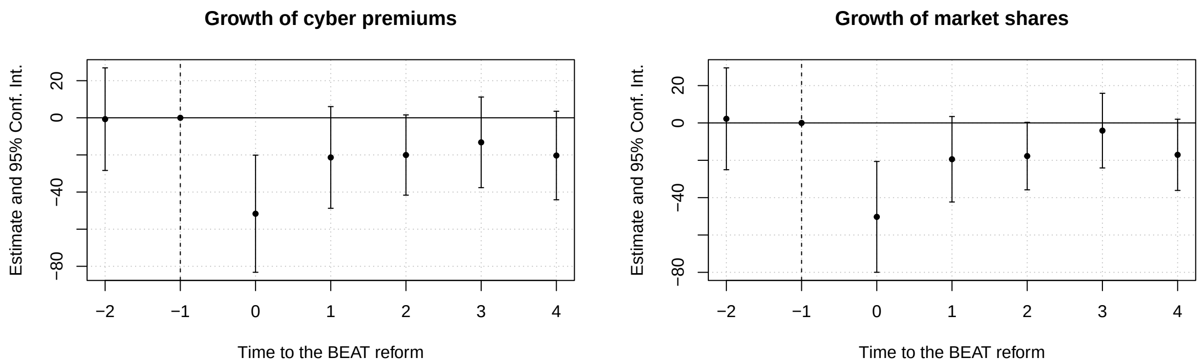

Figure 6: Event study: 2016-2022

Note: The figures report the event study results for the insurers that are affected by BEAT. The control group is the insurers below the threshold of \$500M premiums, and the treatment group includes the ones with premiums higher than \$500M. The dependent variable is the growth rate of cyber premiums for the left figure and the growth rate of market shares for the right figure.

share by line according to the share of premiums of the line in the total premiums of insurers. Thus, the continuous treatment is defined as:

$$D = \frac{DPW_C}{GPW - R_D} * \frac{R_F}{GPW - R_D}, \tag{6}$$

where DPW_C is the direct cyber premiums written by the insurer, GPW is the gross premiums written of all lines by the insurer, R_F is the premiums ceded to non-US affiliates, and R_D is the premiums ceded to US affiliates. As argued in Section 4.2, the use of affiliated reinsurance is closely related inside the rating unit and the impact on the affiliated reinsurance affects all subsidiaries in the same unit, thus we calculate the measure D using rating-unit level data rather than individual company level. We use the difference between GPW and R_D in the denominator because it eliminates the double counting of affiliated reinsurance premiums at the rating unit level (More details can be found in Appendix D). The measure of exposure to the shock, D is calculated using the data in 2017 for each insurer.

The variable $Post$ in Equation 5 is a post-reform dummy. To study the possible long-term effect, we use the dummy variable for the years 2018, 2019, and 2020 and the interaction terms of these dummies and the treatment variable in the regression. The interaction δ

is the coefficient of interest, measuring the effect of BEAT on the supply of cyber insurance. Vector X_{it} is a set of lagged financial variables of the insurers, such as direct premiums written, leverage, and growth of operating incomes of the insurer. τ_t is the time fixed effect, σ_i is a time-invariant firm fixed effect, and ϵ_{it} controls for unobserved factors.

As our dependent variables are the first-order differences (change in premiums, change in market share), we ensure the data are consistent over time to avoid jumps in values. We use the insurers that are affected by BEAT (over \$500 million total premiums), have stable cyber premiums over \$1 million, and have positive premiums ceded to affiliates from 2015 to 2017. Table 7 presents the summary statistics of the variables in Equation (5).

Table 7: Summary statistics for DiD analysis

	N	Mean	St. Dev.	Min	Max
Growth of cyber premiums (%)	288	16.371	41.472	−100.000	104.174
Growth of market share (%)	288	−0.859	43.259	−100.000	104.174
D, Exposure to BEAT	288	20.477	41.408	0.000	147.900
Lag asset (log)	288	13.946	2.019	9.671	17.589
Lag direct premiums (log)	288	13.489	1.258	9.525	15.750
Lag combined ratio (%)	288	75.048	44.124	−5.032	131.391
Lag leverage (%)	288	79.705	65.346	0.000	231.988
Growth of direct premiums	288	7.365	19.838	−94.423	175.110

Note: This table presents the summary statistics of key variables for our DiD estimation. D is the cyber exposure of insurers to the BEAT reform. We winsorize the data at the top 10% to control for the impact of outliers.

Table 8 displays the estimates of the exposure to the tax reform on the growth rate of cyber premiums and market share. The results show that exposure to BEAT reform has a real economic effect on cyber insurers by reducing the growth of cyber insurance premiums and reducing the growth of market shares. In Panel A, the coefficients on the interaction term in 2019 are significantly negative, suggesting that the exogenous shock affects the supply of cyber insurance after one year. In terms of economic magnitude, all else equal, one standard deviation increase of cyber exposure to BEAT leads to a 14.88% decrease in the growth rate of cyber premiums (column 3) and a 16.22% decrease in the growth rate of the market share (column 6) in 2019. The insignificant results in 2020 indicate that the impact is only temporary, as after two years, insurers have enough time to substitute their share of non-US affiliated reinsurance to US affiliated reinsurance or other sources.

Moreover, compared to Figure 6 with immediate negative impact after reform, the negative results are more significant after one year of the reform, i.e. 2019. The possible reason is that all firms are treated in the current results and what we capture is the differences in reform impact due to different levels of exposures, which might take time to reveal.

Panel B provides additional support for Hypothesis 1 by estimating Equation 5 where the treatment group is defined as cyber insurers that rely heavily on non-US affiliated reinsurance, that is, above the median. We find that the effect of the shock becomes even more pronounced. The insurers with high reliance experienced a drop in the growth rate of cyber premiums of 30.36% in 2019 (column 3). The decrease is of similar magnitude to the growth rate of market share.

To further highlight the unique link between the supply of cyber insurance and the availability of affiliated reinsurance, we examine the impact of the BEAT reform on the supply of other types of insurance for the same set of insurers (Hypothesis 2). We follow the specification for the cyber line and calculate the exposure of each insurance line to the BEAT reform for each insurer. Table 9 and 10 present the regression results for 14 different insurance lines. All of the coefficients for these insurance lines are not significant, suggesting that the cyber line is the only business line significantly affected by the shock to the availability of affiliated reinsurance.[9]

7 Which Characteristics of Cyber Risk Prevent Risk Transfer Outside the Insurance Group?

The results show cyber insurance supply is causally affected by the availability of affiliated reinsurance. The significant reliance on the internal market suggests limited access to the external capital market. Otherwise, insurers could readily replace internal capital with external funding. In this section, we analyze which characteristics of the cyber risk, such as heavy tails, information asymmetry, and risk uncertainty, affect the cyber risk transfer to the external reinsurance market.

[9] The financial guarantee line is dropped due to the fact that there are very few insurers underwrite this type of insurance, and thus, very little variation cross-sectionally.

Table 8: The BEAT reform and the supply of cyber insurance

Panel A: Continuous treatment variable						
Dependent variable	Growth of cyber premiums (%)			Growth of market share (%)		
Model	(1)	(2)	(3)	(4)	(5)	(6)
Treat*Y2018	-0.1201	-0.1645	-0.1441	-0.1537	-0.1957	-0.1801
	(0.1359)	(0.1492)	(0.1369)	(0.1541)	(0.1606)	(0.1558)
Treat*Y2019	-0.2680*	-0.3110**	-0.3542*	-0.2774*	-0.3227**	-0.3861**
	(0.1595)	(0.1499)	(0.1863)	(0.1624)	(0.1614)	(0.1873)
Treat*Y2020	0.1378	0.0589	-0.0417	0.1017	0.0228	-0.0944
	(0.1391)	(0.1599)	(0.1902)	(0.1816)	(0.1721)	(0.2337)
Insurer FE	N	N	Y	N	N	Y
Year FE	N	N	Y	N	N	Y
Control	N	Y	Y	N	Y	Y
Observations	288	288	288	288	288	288
R^2	0.06381	0.16234	0.41877	0.02058	0.10820	0.35407

Panel B: Binary treatment variable						
Dependent Variable	Growth of cyber premiums (%)			Growth of market share (%)		
Model	(1)	(2)	(3)	(4)	(5)	(6)
Treat*Y2018	-16.08	-13.82	-14.00	-14.00	-11.74	-11.79
	(9.820)	(12.52)	(9.481)	(11.60)	(13.50)	(11.27)
Treat*Y2019	-28.20**	-26.84**	-30.36**	-27.65**	-26.37*	-30.74**
	(12.15)	(12.53)	(11.80)	(12.75)	(13.50)	(12.53)
Treat*Y2020	-15.34	-16.46	-22.05*	-12.82	-13.84	-19.43
	(13.41)	(12.71)	(12.86)	(13.82)	(13.70)	(13.56)
Insurer FE	N	N	Y	N	N	Y
Year FE	N	N	Y	N	N	Y
Control	N	Y	Y	N	Y	Y
Observations	288	288	288	288	288	288
R^2	0.06363	0.16072	0.42139	0.01807	0.10358	0.35378

Note: This table presents estimates of the impact of the BEAT on the growth rate of cyber premiums and the market share for the insurers. The continuous treatment (exposure to the BEAT reform) in Panel A is calculated as the share of cyber premiums multiplied by the share of non-US affiliated reinsurance in gross premiums written by the insurer. The treatment group in Panel B is defined as the insurers that have exposure to the BEAT reform above the median. Clustered standard errors at the insurer level are reported in parentheses. ***, **, and * denote the statistical significance at the 1%, 5%, and 10% level, respectively.

Table 9: The impact of the BEAT on different lines of businesses; dependent variable: growth rate of direct premiums written (%)

Model	Accident & health (1)	Homeowner (2)	Auto damage (3)	Fire (4)	Multi-peril (5)	Financial (6)	Marine (7)
Treat*Y2018	-0.0084	-0.6200	0.0540	-0.0074	0.0065	-	-0.1245
	(0.0408)	(0.7090)	(0.0637)	(0.0382)	(0.0348)	-	(0.1220)
Treat*Y2019	-0.0638	-1.027	0.0819	0.0038	-0.0125	-	-0.0982
	(0.0570)	(0.8845)	(0.0556)	(0.0350)	(0.0357)	-	(0.0874)
Treat*Y2020	-0.1360	-0.8985	0.1509	0.0372	-0.0154	-	-0.1152
	(0.1315)	(0.6860)	(0.2290)	(0.0416)	(0.0313)	-	(0.1222)
Insurer FE	Y	Y	Y	Y	Y	Y	Y
Year FE	Y	Y	Y	Y	Y	Y	Y
Control	Y	Y	Y	Y	Y	Y	Y
Observations	256	285	269	266	244	-	266
R^2	0.21451	0.40283	0.28009	0.21883	0.38960	-	0.19021

Model	Medical liability (8)	Workers' comp (9)	Other liability (10)	Auto liability (11)	Aircraft (12)	Fidelity (13)	Other (14)
Treat*Y2018	-0.1012	0.0809	0.0047	-0.1370	-0.2529	-0.1939	0.7242
	(0.2431)	(0.0670)	(0.0062)	(0.1063)	(0.3373)	(0.1981)	(0.7379)
Treat*Y2019	0.2539	0.0112	0.0076	-0.0562	-0.2131	-0.0607	0.5628
	(0.2587)	(0.0719)	(0.0069)	(0.0611)	(0.3364)	(0.1271)	(0.6405)
Treat*Y2020	-0.0369	-0.1448	0.0007	0.1101	-0.2606	-0.6843	0.5513
	(0.3945)	(0.1686)	(0.0039)	(0.2263)	(0.2561)	(0.6868)	(0.6891)
Insurer FE	Y	Y	Y	Y	Y	Y	Y
Year FE	Y	Y	Y	Y	Y	Y	Y
Control	Y	Y	Y	Y	Y	Y	Y
Observations	240	255	268	252	276	189	236
R^2	0.31038	0.28164	0.42216	0.22224	0.35976	0.21970	0.21779

Note: This table presents estimates of the impact of the BEAT on the growth rate of direct premiums written by different lines of businesses. The treatment is the continuous variable, calculated as the share of each line's premiums multiplied by the share of non-US affiliated reinsurance in gross premiums written by the insurer. Insurer and year-fixed effects are controlled for all regressions. Clustered standard errors at the insurer level are reported in parentheses. There is no result for financial guarantee line due to limited observations. A detailed definition of each line of business is provided in Appendix B. ***, **, and * denote the statistical significance at the 1%, 5%, and 10% levels, respectively.

Table 10: The impact of the BEAT on different lines of businesses; dependent variable: growth rate of market share (%)

Model	Accident & health (1)	Homeowner (2)	Auto damage (3)	Fire (4)	Multi-peril (5)	Financial (6)	Marine (7)
Treat*Y2018	0.0027	-0.5896	0.0539	-0.0067	0.0061	-	-0.1238
	(0.0388)	(0.7042)	(0.0606)	(0.0376)	(0.0345)	-	(0.1179)
Treat*Y2019	-0.0607	-1.036	0.0821	0.0043	-0.0129	-	-0.0974
	(0.0573)	(0.8820)	(0.0523)	(0.0340)	(0.0356)	-	(0.0867)
Treat*Y2020	-0.1030	-0.8919	0.1542	0.0339	-0.0153	-	-0.1142
	(0.1242)	(0.6785)	(0.2360)	(0.0406)	(0.0311)	-	(0.1230)
Insurer FE	Y	Y	Y	Y	Y	Y	Y
Year FE	Y	Y	Y	Y	Y	Y	Y
Control	Y	Y	Y	Y	Y	Y	Y
Observations	256	285	269	266	244	-	266
R^2	0.22001	0.39832	0.27194	0.22653	0.38433	-	0.19054

Model	Medical liability (8)	Workers' comp (9)	Other liability (10)	Auto liability (11)	Aircraft (12)	Fidelity (13)	Other (14)
Treat*Y2018	-0.0997	0.0756	0.0048	-0.1344	-0.2597	-0.1845	0.7222
	(0.2421)	(0.0675)	(0.0061)	(0.1039)	(0.3426)	(0.1902)	(0.7366)
Treat*Y2019	0.2320	0.0149	0.0075	-0.0557	-0.2468	-0.0558	0.5623
	(0.2520)	(0.0731)	(0.0068)	(0.0589)	(0.3406)	(0.1230)	(0.6387)
Treat*Y2020	-0.0442	-0.1311	0.0004	0.1148	-0.3078	-0.6861	0.5492
Insurer FE	Y	Y	Y	Y	Y	Y	Y
Year FE	Y	Y	Y	Y	Y	Y	Y
Control	Y	Y	Y	Y	Y	Y	Y
Observations	240	255	268	252	276	189	236
R^2	0.31110	0.28620	0.42539	0.22041	0.34865	0.22131	0.21770

Note: This table presents estimates of the impact of the BEAT on the growth rate of market share by different lines of businesses. The treatment is the continuous variable, calculated as the share of each line's premiums multiplied by the share of non-US affiliated reinsurance in gross premiums written by the insurer. Insurer and year-fixed effects are controlled for all regressions. Clustered standard errors at the insurer level are reported in parentheses. There is no result for financial guarantee line due to limited observations. A detailed definition of each line of business is provided in Appendix B. ***, **, and * denote the statistical significance at the 1%, 5%, and 10% levels, respectively.

7.1 Heavy tails

Heavy-tailedness is an important property of cyber risk and this may affect the risk transfer to reinsurers as cyber insurance is exposed to more extreme risks than other insurance lines. Empirically, this indicates that the price of cyber reinsurance is higher than other types of reinsurance to compensate for the additional risk. However, as there is no data available for cyber reinsurance, one possibility is to estimate its use by considering the share of cyber premiums.

As standalone cyber policies are categorized into the other liability line and package policies into the commercial multi-peril line, we use the share of cyber premiums in each line as a proxy for the share of reinsurance, assuming that the reinsurance usage is proportional to premiums written.[10] Therefore, the share of cyber premiums is positively related to the price of reinsurance for the whole line of business, because a higher share indicates more cyber exposure being reinsured, which results in a higher reinsurance price.

7.2 Risk uncertainty

As cyber risk is constantly evolving, it is difficult to accurately measure the cyber exposure in the portfolio. Thus, insurers with more expertise in the underwriting of cyber risk may have a competitive advantage in estimating cyber exposure and negotiating reinsurance prices. To measure the level of expertise in cyber risk of different insurers, we use the data from the System for Electronic Rates and Forms Filing, which collects all the insurance product filings in the US. Theoretically, the standalone cyber products are categorized into the other liability line, and package products are categorized into the commercial multi–peril line, but this is not perfectly implemented in practice and there are still cyber policies that spread across different lines of businesses. Therefore, we use text mining together with GPT API to identify the cyber products. The idea is to check the filing description of each record, which typically summarizes the purpose and content of the filing. This description provides enough information to identify whether the submission is related to

[10] This might be a lower bound of the cyber reinsurance as insurers tend to transfer more risky businesses to reinsurers.

cyber products. GPT API is an efficient tool for this purpose, and it achieves more than 90% accuracy in our manually generated training sample. We filtered the initial sample of more than 100,000 filings from 2013 to 2022, achieving 1,372 filings that are relevant to our analysis.

We consider the number of pages and filing frequency of cyber products as a proxy for the level of cyber knowledge/experience of one insurer. Intuitively, the insurer with more knowledge could provide more detailed risk classification and price differentiation for different customers, this would require a higher number of pages to describe the product and a higher frequency of updating their products. However, after the manual check, we find that the number of pages as a proxy has large noises as it does not necessarily indicate the level of expertise of the insurer. For example, across different insurers, it is not standardized what types of forms are filed for approval within each cyber product. Therefore, some insurers have a higher number of pages because they include more administrative forms (with little relevant information) that are not filed by other insurers. In addition, for package policies, it is common that the cyber coverages are filed together with other coverages, thus blurring the relevance of such filings for our purpose. Therefore, the filing frequency of cyber products is a more informative proxy to measure the experience of cyber underwriting of the insurer.

7.3 Information asymmetry

Directly measuring information asymmetry in the reinsurance market is challenging. Doherty and Smetters (2005) propose an indirect measure, as reinsurers use price incentives and monitoring in the long-term insurance contract to limit moral hazard in the presence of information asymmetry. Therefore, we can empirically test the use of experience rating, monitoring, and direct price control to provide evidence on the severity of information asymmetry issues in the market.

The dependent variable is the price of reinsurance, but there is no direct measure. Therefore, we consider the ratio of reinsurance premiums over the reinsured losses for insurer i at time t, which is similar to the estimation for primary insurance in Table 2.

Experience rating is measured by the ratio of direct premiums to direct losses. If reinsurers "experience rate" the past losses to control for moral hazard, high past losses (low premium-to-loss ratio) would lead to high current prices. Thus, the relationship between this measure and the reinsurance price is predicted to be negative. However, cross-sectionally, this ratio can be positively related to the dependent variable as the firms with high past losses tend to have high reinsured losses (the inverse of the reinsurance price).

Monitoring is proxied by the share of reinsured losses in total losses, as there is no direct measure. The reason we use such a proxy for monitoring is that investment in monitoring is reflected in prices and it increases in the share of reinsured losses. Therefore, the relationship between this variable and the reinsurance price should be positive if monitoring is in place. Lastly, direct price control is measured by experience rating multiplied by the share of reinsured losses as the sensitivity of prices to past losses increases as more losses are reinsured. The relationship between the dependent variable and the price control is predicted to be negative when reinsurers use direct price control.

7.4 Empirical specification and results

We aim to estimate how the reinsurance price depends on various factors discussed above. To this end, we measure the correlation between the price of reinsurance and the empirical measures of heavy tails, risk uncertainty, and information asymmetry. To calculate the price for external reinsurance, we need to distinguish between affiliated and non-affiliated reinsurance, but there is no data for this purpose. Therefore, we use the share of non-affiliated reinsurance in total reinsurance as a proxy, which estimates the difference in prices between these two types of reinsurance. To understand how the issue of information asymmetry is related to cyber insurance, we use the interaction terms of information asymmetry measures with the share of cyber premiums. Furthermore, we also include the interaction terms with the share of non-affiliated reinsurance to estimate the severity of information asymmetry issues for different levels of non-affiliated reinsurance usage. Therefore, there are interaction terms with at most three variables. The empirical specification is as follows:

$$
\begin{aligned}
Reinsurance\,price_t = \alpha + \underbrace{\beta \cdot cybershare_{t-1}}_{\text{Heavy tail}} + \underbrace{\gamma \cdot non\,aff_{t-1}}_{\text{Non-affiliated reinsurance}} + \underbrace{\lambda \cdot update\,freq_{t-1}}_{\text{Risk uncertainty}} \\
\underbrace{\epsilon \cdot control_{t-1} + \delta \cdot exp\_rate_{t-1} + \omega \cdot monitor_{t-1}}_{\text{Info asymmetry}} + \\
\underbrace{cybershare_{t-1} \cdot non\,aff_{t-1} \cdot (\epsilon 1 \cdot control_{t-1} + \delta 1 \cdot exp\_rate_{t-1} + \omega 1 \cdot monitor_{t-1})}_{\text{Info asymmetry for lines with cyber insurance and non-aff reinsurance}} + \\
\underbrace{\lambda 1 \cdot cybershare_{t-1} \cdot non\,aff_{t-1} \cdot update\,freq_{t-1}}_{\text{Risk uncertainty for lines with cyber insurance and non-aff reinsurance}} + other\ interaction\ terms,
\end{aligned}
\tag{7}
$$

where *cybershare* is the share of cyber insurance in the corresponding line of business, *non aff* is the share of non-affiliated reinsurance, and *update freq* is the number of updates for cyber products since 2013. Direct price control *control*, experience rating *exp_rate*, and monitoring *monitor* are the measures of information asymmetry. The interaction terms with three variables such as $cybershare_{t-1} \cdot non\,aff_{t-1} \cdot control_{t-1}$ estimate the effects of information asymmetry and risk uncertainty for lines with cyber insurance and non-affiliated reinsurance. *other interaction terms* include all interaction terms among *cybershare*, *non aff*, and the measures of information asymmetry and risk uncertainty. We refer to Table 11 for the summary of the factors affecting the reinsurance prices and their economic interpretations.

We use the data at the rating unit level and focus on insurance groups with more than $500 million in gross premiums written. As we argue in Section 4.2, the reinsurance decisions are likely coordinated inside the rating unit and thus it is more reasonable to aggregate reinsurance data to rating unit level for the analysis of the reinsurance usage and prices. We do not restrict the sample based on cyber premiums, as we consider the insurers with or without cyber exposures. Table 12 presents the summary statistics of key variables used in our analysis for the other liability line and multi-peril line.

Table 13 reports the regression results. For standalone policies (columns 1-3), the coefficients for the share of cyber insurance and non-affiliated reinsurance are significantly

Table 11: Interpretation: Factor decomposition of cyber reinsurance price

non_aff	reinsurance price reaction to the share of external reinsurance (+, **external reinsurance is more expensive**)
cybershare	reinsurance price reaction to the share of cyber insurance (+, **cyber reinsurance is more expensive**)
exp_rate	reinsurance price reaction to experience rating or past losses (–, **experience rating is used by reinsurers**)
monitor	reinsurance price reaction to the monitoring efforts (+, **monitoring is used by reinsurers**)
control	reinsurance price reaction to the direct control (–, **direct price control is effective as it increases the sensitivity of reinsurance price to experience rating**)
update_freq	reinsurance price reaction to update frequency (–, **higher frequency reduces reinsurance prices**)
cybershare × update_freq	reinsurance price reaction to update frequency given the level of cyber share (–, **higher update frequency leads to a lower price when the cyber share is higher**)
non_aff × update_freq	reinsurance price reaction to update frequency given the level of non-affiliated reinsurance (–, **higher update frequency leads to a lower price when non-affiliated reinsurance is higher**)
non_aff × cybershare × exp_rate	reinsurance price reaction to experience rating given the level of non-affiliated reinsurance and cyber insurance shares (–, **experience rating is used more intensively with more non-affiliated reinsurance and cyber insurance**)
non_aff × cybershare × monitor	reinsurance price reaction to monitoring efforts given the level of non-affiliated reinsurance and cyber insurance shares (+, **with more non-affiliated reinsurance and cyber insurance, the effect of monitoring on reinsurance price is higher**)
non_aff × cybershare × control	reinsurance price reaction to direct price control given the level of non-affiliated reinsurance and cyber insurance shares (–, **with more non-affiliated reinsurance and cyber insurance, the sensitivity of price to direct price control is higher**)
non_aff × cybershare × update_freq	reinsurance price reaction to update frequency given the level of non-affiliated reinsurance and cyber insurance shares (–, **with more non-affiliated reinsurance and cyber insurance, the update frequency of cyber insurer reduces more significantly the reinsurance prices**)

Note: This table presents the interpretation of key terms in Equation 7 and the predicted signs of the coefficients.

positive, which provides evidence that higher exposure to cyber insurance and the use of non-affiliated reinsurance lead to higher reinsurance prices. More specifically, a 1% increase in the use of non-affiliated reinsurance relates to a 0.4% increase in reinsurance price cross-sectionally (column 2), assuming the insurers have average characteristics in other dimensions. The effect of cyber insurance on reinsurance price is much stronger, given an insurer with average characteristics, a 1% increase in the share of cyber insurance is associated with a 41.5% increase in reinsurance price (column 3).

Furthermore, the interaction term *non-aff* × *cybershare* × *monitor* is positive, and *non-aff* × *cybershare* × *control* is negative, indicating that information asymmetry issues are more significant for insurers with more cyber exposure and use of external reinsurance. The results for package policies (columns 4–6) are mostly not significant, indicating information asymmetry and heavy tails are not decisive factors for this market. But the interaction term *non-aff* × *update_freq* is negative, which is consistent with the argument that high update frequency of cyber products reduce the reinsurance price when the insurer uses more non-affiliated reinsurance.

In general, the results show that all three factors play a role in affecting the reinsurance price and thus limiting the access to the external capital for cyber insurers. In particular, the effects are stronger for the standalone segment than the package segment.

8 Conclusion

In this paper, we investigate the supply of cyber insurance and argue that it is characterized by a combination of unique features — heavy tails, uncertain loss distribution, and information asymmetries. These features create the need to finance tail exposures by holding more capital while also increasing the wedge between the cost of internal and external capital. This results in a situation in which insurers heavily rely on ICM in the form of affiliated reinsurance. Further, we establish a causal link using the regulatory change in the taxation of the non-US affiliated reinsurance as identification. We find that insurers reduce their supply of cyber insurance in response to the shock. We then analyze factors that drive the cost of external capital and show that all of the features of cyber risk play

Table 12: Summary statistics

Statistic	N	Mean	St. Dev.	Min	Max
Other liability line					
cybershare	720	0.383	1.483	0.000	14.344
non-aff	720	46.288	37.327	0.000	100.000
price	720	1.672	2.042	0.016	18.436
exp_rate	720	1.550	1.213	0.016	9.110
monitor	720	0.549	0.292	0.0002	1.000
control	720	0.841	0.841	0.0003	7.208
update_freq	720	1.732	2.954	0	22
Commericial multi-peril line					
cybershare	597	1.998	7.989	0.000	97.842
non-aff	597	42.063	36.275	0.000	100.000
price	597	1.600	1.944	0.001	18.683
exp_rate	597	1.346	0.855	0.007	9.517
monitor	597	0.492	0.325	0.001	1.000
control	597	0.656	0.737	0.001	7.830
update_freq	597	1.851	2.724	0	16

Note: This table presents the summary statistics for the variables in our sample. *cybershare (%)* is the percentage of cyber premiums in the total premiums written in the other liability line or the multi-peril line. *non-aff (%)* is the percentage of reinsurance premiums that are ceded to non-affiliated reinsurance. *price* is the reinsurance price, exp_rate is the experience rating, *monitor* is the variable for monitoring, and *control* is the variable for direct price control. *update_freq* is the cumulative number of updates of cyber products for the insurer from the year 2013 (the start of our sample period).

Table 13: Factor decomposition of cyber reinsurance price

Dependent Variable	Reinsurance price					
	Other liability line			Commericial multi-peril line		
Model	(1)	(2)	(3)	(4)	(5)	(6)
non-aff	0.0249**	0.0234***	0.0132	-0.0002	0.0003	0.0108
	(0.0102)	(0.0056)	(0.0204)	(0.0132)	(0.0087)	(0.0168)
cybershare	1.332	1.309	2.824***	-0.1275	-0.1387	0.0931
	(0.9208)	(0.9261)	(0.8556)	(0.1647)	(0.2535)	(0.1423)
exp_rate	1.676***	1.629***	0.3296	0.3903	0.3942	1.596
	(0.2185)	(0.1415)	(0.5106)	(0.8103)	(0.3714)	(1.177)
monitor	0.9114	0.7559	-0.1353	-1.094	-1.158	-0.7165
	(0.5984)	(0.5578)	(1.300)	(1.261)	(0.7838)	(1.960)
control	-1.368***	-1.306***	-0.1371	-0.2718	-0.2830	-1.242
	(0.3256)	(0.2410)	(0.6625)	(0.9290)	(0.4853)	(1.327)
update_freq	0.0103	0.0114	-0.0053	0.0215	0.0331	0.0676
	(0.0408)	(0.0353)	(0.0585)	(0.0294)	(0.0453)	(0.0622)
non-aff × cybershare	-0.0308	-0.0294	-0.0738**	-8×10^{-5}	0.0003	-0.0013
	(0.0230)	(0.0182)	(0.0327)	(0.0020)	(0.0032)	(0.0015)
cybershare × exp_rate	-1.234*	-1.165**	-2.042***	0.0147	0.0406	-0.0783
	(0.6545)	(0.4961)	(0.6971)	(0.1116)	(0.1334)	(0.0791)
cybershare × monitor	-1.824	-1.908	-5.020***	0.1092	0.1452	-0.0235
	(1.548)	(1.973)	(1.319)	(0.1843)	(0.2931)	(0.1495)
cybershare × control	1.653*	1.635*	3.356***	0.0088	-0.0335	0.0671
	(0.9612)	(0.9852)	(0.8540)	(0.1318)	(0.1735)	(0.0893)
non-aff × exp_rate	-0.0119**	-0.0115***	-0.0055	0.0034	0.0027	-0.0122
	(0.0059)	(0.0026)	(0.0104)	(0.0105)	(0.0053)	(0.0121)
non-aff × monitor	-0.0272*	-0.0254***	-0.0141	-0.0014	-0.0036	0.0026
	(0.0138)	(0.0086)	(0.0242)	(0.0153)	(0.0129)	(0.0197)
non-aff × control	0.0136*	0.0129***	0.0049	-0.0029	-0.0017	0.0096
	(0.0079)	(0.0040)	(0.0126)	(0.0118)	(0.0069)	(0.0135)
cybershare × update_freq	0.0049	0.0052	0.0212	0.0063	0.0034	-0.0057
	(0.0196)	(0.0501)	(0.0178)	(0.0045)	(0.0115)	(0.0060)
non-aff × update_freq	-0.0003	-0.0003	0.0001	-0.0041***	-0.0042***	-0.0011
	(0.0018)	(0.0009)	(0.0018)	(0.0015)	(0.0013)	(0.0013)
non-aff × cybershare × exp_rate	0.0265	0.0249*	0.0629*	0.0003	-2.22×10^{-5}	0.0011
	(0.0198)	(0.0138)	(0.0320)	(0.0015)	(0.0018)	(0.0009)
non-aff × cybershare × monitor	0.0421	0.0408	0.1172***	0.0014	0.0008	0.0012
	(0.0330)	(0.0350)	(0.0448)	(0.0024)	(0.0043)	(0.0017)
non-aff × cybershare × control	-0.0351	-0.0335	-0.0955**	-0.0016	-0.0009	-0.0016
	(0.0259)	(0.0220)	(0.0433)	(0.0021)	(0.0032)	(0.0013)
non-aff × cybershare × update_freq	-0.0003	-0.0002	-0.0004	7.11×10^{-5}	6.77×10^{-5}	5.26×10^{-5}
	(0.0004)	(0.0010)	(0.0003)	(7.08×10^{-5})	(0.0002)	(7.85×10^{-5})
Controls	No	Yes	Yes	No	Yes	Yes
Firm	No	No	Yes	No	No	Yes
Year	No	Yes	Yes	No	Yes	Yes
Observations	720	720	720	597	597	597
R^2	0.32849	0.34051	0.62496	0.14714	0.16715	0.56073

Note: This table presents the results for the factor decomposition of reinsurance price in the other liability line. Column (1) to (3) are the results for affiliated reinsurance, and Column (4) to (6) are the results for non-affiliated reinsurance. Column (1) and (4) do not include controls and fixed effects, Column (2) and (5) include controls and year fixed effects, Column (3) and (6) include controls and firm-year fixed effects. Clustered standard errors at the insurance group level are reported in parentheses. ***, **, and * denote the statistical significance at the 1%, 5%, and 10% level, respectively.

a role.

Our findings imply that the growth of the cyber insurance market is constrained by supply-side factors, and it is challenging for the insurance market alone to provide sufficient coverage for cyber risk. These observations suggest that both public and private sectors are to play a role in protecting the economies from cyber risk. The design of such partnerships is a policy-relevant topic that we leave for future research.

References

Aldasoro, I., L. Gambacorta, P. Giudici, and T. Leach. 2022. The drivers of cyber risk. *Journal of Financial Stability* 60:100989–.

Baker, T., and A. Shortland. 2023. Insurance and enterprise: Cyber insurance for ransomware. *The Geneva Papers on Risk and Insurance-Issues and Practice* 48:275–99.

Barth, M. M., and D. L. Eckles. 2009. An empirical investigation of the effect of growth on short-term changes in loss ratios. *Journal of Risk and Insurance* 76:867–85.

Berry-Stölzle, T. R., and P. Born. 2012. The effect of regulation on insurance pricing: The case of Germany. *Journal of Risk and Insurance* 79:129–64.

Borch, K. 1962. Equilibrium in a reinsurance market. *Econometrica* 30:424–44.

Cebula, J. L., and L. R. Young. 2010. A taxonomy of operational cyber security risks. Working Paper, Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.

Crosignani, M., M. Macchiavelli, and A. F. Silva. 2023. Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics* 147:432–48.

Cummins, J. D., and M. A. Weiss. 2016. Equity capital, internal capital markets, and optimal capital structure in the US property-casualty insurance industry. *Annual Review of Financial Economics* 8:121–53.

Diamond, D. W. 1994. Corporate capital structure: The control roles of bank and public debt with taxes and costly bankruptcy. *FRB Richmond Economic Quarterly* 80:11–37.

Doherty, N., and K. Smetters. 2005. Moral hazard in reinsurance markets. *Journal of Risk and Insurance* 72:375–91.

Doherty, N. A. 1997. Financial innovation in the management of catastrophe risk. *Journal of Applied Corporate Finance* 10:84–95.

Doherty, N. A., and H. Schlesinger. 1990. Rational insurance purchasing: Consideration of contract nonperformance. *Quarterly Journal of Economics* 105:243–53.

Edwards, B., S. Hofmeyr, and S. Forrest. 2016. Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity* 2:3–14.

Eisenbach, T. M., A. Kovner, and M. J. Lee. 2022. Cyber risk and the US financial system: A pre-mortem analysis. *Journal of Financial Economics* 145:802–26.

Eling, M., R. Ibragimov, and D. Ning. 2023. Time dynamics of cyber risk. *Available at SSRN 4497621* .

Eling, M., and N. Loperfido. 2017. Data breaches: Goodness of fit, pricing, and risk measurement. *Insurance: Mathematics and Economics* 75:126–36.

Eling, M., and J. Wirfs. 2019. What are the actual costs of cyber risk events? *European Journal of Operational Research* 272:1109–19.

Falco, G., M. Eling, D. Jablanski, M. Weber, V. Miller, L. A. Gordon, S. S. Wang, J. Schmit, R. Thomas, M. Elvedi, et al. 2019. Cyber risk research impeded by disciplinary barriers. *Science* 366:1066–9.

Farkas, S., O. Lopez, and M. Thomas. 2021. Cyber claim analysis using generalized pareto regression trees with applications to insurance. *Insurance: Mathematics and Economics* 98:92–105.

Fier, S. G., K. A. McCullough, and J. M. Carson. 2013. Internal capital markets and the partial adjustment of leverage. *Journal of Banking & Finance* 37:1029–39.

Florackis, C., C. Louca, R. Michaely, and M. Weber. 2023. Cybersecurity risk. *Review of Financial Studies* 36:351–407.

Foerderer, J., and S. W. Schuetz. 2022. Data breach announcements and stock market reactions: a matter of timing? *Management Science* 68:7298–322.

Froot, K. A. 2001. The market for catastrophe risk: A clinical examination. *Journal of Financial Economics* 60:529–71.

———. 2007. Risk management, capital budgeting, and capital structure policy for insurers and reinsurers. *Journal of Risk and Insurance* 74:273–99.

Froot, K. A., and P. G. O'Connell. 2008. On the pricing of intermediated risks: Theory and application to catastrophe reinsurance. *Journal of Banking & Finance* 32:69–85.

Froot, K. A., D. S. Scharfstein, and J. C. Stein. 1993. Risk management: Coordinating corporate investment and financing policies. *Journal of Finance* 48:1629–58.

Froot, K. A., and J. C. Stein. 1998. Risk management, capital budgeting, and capital structure policy for financial institutions: An integrated approach. *Journal of Financial Economics* 47:55–82.

Garven, J. R., and J. Lamm-Tennant. 2003. The demand for reinsurance: Theory and empirical tests. *Insurance and Risk Management* 7:217–37.

Ge, S. 2022. How do financial constraints affect product pricing? Evidence from weather and life insurance premiums. *Journal of Finance* 77:449–503.

Gertner, R. H., D. S. Scharfstein, and J. C. Stein. 1994. Internal versus external capital markets. *Quarterly Journal of Economics* 109:1211–30.

Gründl, H., D. Guxha, A. Kartasheva, and H. Schmeiser. 2021. Insurability of pandemic risks. *Journal of Risk and Insurance* 88:863–902.

Harrington, S. E. 2004. Effects of prior approval rate regulation of auto. *Deregulating Property-Liability Insurance: Restoring Competition and Increasing Market Efficiency* 285–314.

Ibragimov, R., D. Jaffee, and J. Walden. 2009. Nondiversification traps in catastrophe insurance markets. *Review of Financial Studies* 22:959–93.

Jaffee, D. M., and T. Russell. 1997. Catastrophe insurance, capital markets, and uninsurable risks. *Journal of Risk and Insurance* 64:205–30.

Kamiya, S., J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz. 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics* 139:719–49.

Koijen, R. S., and M. Yogo. 2015. The cost of financial frictions for life insurers. *American Economic Review* 105:445–75.

———. 2022. The fragility of market risk insurance. *Journal of Finance* 77:815–62.

Luciano, E., and G. Nicodano. 2014. Guarantees, leverage, and taxes. *Review of Financial Studies* 27:2736–72.

Malavasi, M., G. W. Peters, P. V. Shevchenko, S. Trück, J. Jang, and G. Sofronov. 2022. Cyber risk frequency, severity and insurance viability. *Insurance: Mathematics and Economics* 106:90–114.

McAfee. 2020. The hidden costs of cybercrime. https://companies.mybroadband.co.za/axiz/files/2021/02/eBook-Axiz-McAfee-hidden-costs-of-cybercrime.pdf.

NAIC. 1998. Underwriting pools and associations including intercompany pools. *National Association of Insurance Commissioners Statutory Issue Paper No. 97* .

———. 2016. Report on cyber insurance market. https://content.naic.org/sites/default/files/inline-files/committees_ex_cybersecurity_tf_report_cyber_supplement_0.pdf.

———. 2021. Report on cyber insurance market. https://content.naic.org/sites/default/files/inline-files/cmte-c-report-cybersecurity-insurance-market-211020.pdf.

———. 2022. Report on cyber insurance market. https://content.naic.org/sites/default/files/cmte-c-cyber-supplement-report-2022-for-data-year-2021.pdf.

———. 2023. Report on cyber insurance market. https://content.naic.org/sites/default/files/inline-files/Final%202023%20Cyber%20Report.pdf.

Nicodano, G., and L. Regis. 2019. A trade-off theory of ownership and capital structure. *Journal of Financial Economics* 131:715–35.

Niehaus, G. 2018. Managing capital via internal capital market transactions: The case of life insurers. *Journal of Risk and Insurance* 85:69–106.

Plantin, G. 2006. Does reinsurance need reinsurers? *Journal of Risk and Insurance* 73:153–68.

Powell, L. S., and D. W. Sommer. 2007. Internal versus external capital markets in the insurance industry: The role of reinsurance. *Journal of Financial Services Research* 31:173–88.

Powell, L. S., D. W. Sommer, and D. L. Eckles. 2008. The role of internal capital markets in financial intermediaries: Evidence from insurer groups. *Journal of Risk and Insurance* 75:439–61.

Romanosky, S. 2016. Examining the costs and causes of cyber incidents. *Journal of Cybersecurity* 2:121–35.

Romanosky, S., L. Ablon, A. Kuehn, and T. Jones. 2019. Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity* 5:tyz002–.

Stein, J. C. 2002. Information production and capital allocation: Decentralized versus hierarchical firms. *Journal of Finance* 57:1891–921.

Swiss Re Institute. 2022. Cyber insurance: strengthening resilience for the digital transformation. https://www.swissre.com/institute/research/ topics-and-risk-dialogues/digital-business-model-and-cyber-risk/ cyber-insurance-strengthening-resilience.html.

Woods, D. W., and R. Böhme. 2021a. How cyber insurance shapes incident response: A mixed methods study. In *Workshop on the Economics of Information Security*.

———. 2021b. Sok: Quantifying cyber risk. In *2021 IEEE Symposium on Security and Privacy (SP)*, 211–28. IEEE.

Woods, D. W., T. Moore, and A. C. Simpson. 2021. The county fair cyber loss distribution: Drawing inferences from insurance prices. *Digital Threats: Research and Practice* 2:1–21.

Table 14: Summary statistics for Identity theft insurance market

Year	Premiums (billion $)	Insurers	Insurance groups	Number of policies (million)	Claims frequency (%)	Cyber insurance market share (%)	Combined loss ratio (%)	Standard deviation of loss ratio
Identity theft package policy								
2015	0.21	282	90	11.21	0.00	0.04	0.00	1.66
2016	0.19	292	99	13.50	0.00	0.03	0.00	17.23
2017	0.20	353	118	12.93	0.00	0.03	0.00	1.66
2018	0.21	374	124	14.15	0.00	0.03	0.00	1.10
2019	0.21	388	128	12.61	0.01	0.03	0.00	0.32
2020	0.22	405	136	13.53	0.06	0.03	0.00	1.26
2021	0.23	388	132	13.47	0.00	0.03	0.00	3.92
2022	0.24	388	134	13.61	0.00	0.03	0.00	1.33
Identity theft Standalone Policy								
2015	0.02	14	9	0.50	0.01	0.00	1.45	32.76
2016	0.02	14	8	0.28	0.02	0.00	0.00	33.65
2017	0.02	15	9	0.23	0.02	0.00	0.00	92.72
2018	0.01	18	10	0.24	0.01	0.00	0.00	113.54
2019	0.01	18	9	0.31	0.00	0.00	0.00	8.58
2020	0.01	15	7	0.30	0.00	0.00	0.00	34.62
2021	0.01	14	8	0.28	0.01	0.00	15.37	39.14
2022	0.01	17	7	0.10	0.00	0.00	0.83	29.28

Note: This table presents summary statistics of key variables in the cyber insurance market by year. *Premiums* are calculated as the summation of cyber premiums of all insurers in the respective segment. The number of insurance groups includes independent insurance companies without group affiliation. *Claims frequency* is calculated as the total number of claims divided by the total number of policies in the respective segment. *Cyber insurance market share* is calculated as the cyber premiums of all insurers divided by the total premiums of all insurers. *Combined loss ratio* is the cyber loss incurred plus direct defense and cost containment expense (also known as allocated loss adjustment expense) divided by cyber premiums earned for each insurer and the mean value is reported in this table. The last two columns are calculated after winterizing the top and bottom 1%, as the extreme values significantly distort the statistics.

Appendix A

This appendix provides the basic descriptive statistics for the identity theft segment of the market. Table 14 shows that the identity theft market is negligible measured by market size and has been stagnant over time.

Appendix B

The abbreviations for lines of businesses in this paper are defined as (from S&P Global Market Intelligence, S&P MI):

- Accident & health: accident insurance and health insurance lines
- Homeowner: homeowners and farmowners' multiple peril insurance
- Auto damage: private passenger auto insurance
- Fire: fire and allied lines combined
- Multi–peril: commercial multiple peril insurance
- Financial: financial and mortgage guaranty insurance
- Marine: marine lines combined
- Medical liability: medical professional liability insurance
- Workers' comp: workers' compensation
- Other liability: other liability and product liability insurance combined
- Auto liability: commercial auto liability insurance
- Aircraft: aircraft insurance (all perils)
- Fidelity: fidelity and surety insurance
- Other: other commercial insurance

Appendix C

This section presents the DID results for the impact of the BEAT reform on the supply of cyber insurance using level measures rather than first-order differences. We consider the changes in absolute measures for cyber premiums and market shares rather than the growth measures in the main results. Table 15 reports the results. There is no strong evidence of a significant negative impact on cyber insurance supply. The reason is that the whole market is increasing during the sample period, and the insurers affected by the BEAT reform are also the leading insurers in the market with a rapid growth rate. Therefore, the real effect is reflected more significantly in the first-order differences of premiums and market shares.

Table 15: The BEAT reform and the supply of cyber insurance (level measures)

Panel A: Continuous treatment variable						
Dependent Variable:	Cyber premiums (log)			Market share (%)		
Model:	(1)	(2)	(3)	(4)	(5)	(6)
did1	-0.0002	-0.0015	-0.0021	0.0017	0.0018	0.0022
	(0.0020)	(0.0055)	(0.0026)	(0.0024)	(0.0058)	(0.0025)
did2	-0.0083	-0.0097*	-0.0097	0.0006	-0.0009	-0.0002
	(0.0097)	(0.0056)	(0.0108)	(0.0026)	(0.0058)	(0.0029)
did3	0.0034	-0.0004	-0.0039	0.0047	0.0020	0.0012
	(0.0042)	(0.0059)	(0.0053)	(0.0042)	(0.0062)	(0.0035)
Insurer FE	N	N	Y	N	N	Y
Year FE	N	N	Y	N	N	Y
Control	N	Y	Y	N	Y	Y
Observations	288	288	288	288	288	288
R^2	0.05588	0.30502	0.77925	0.05553	0.20179	0.87421

Panel B: Binary treatment variable						
Dependent Variable:	Cyber premiums (log)			Market share (%)		
Model:	(1)	(2)	(3)	(4)	(5)	(6)
did1	0.0298	0.0666	-0.0160	0.2468	0.2313	0.2467
	(0.1588)	(0.4733)	(0.1615)	(0.2053)	(0.4949)	(0.1970)
did2	-0.4108	-0.3172	-0.2755	0.1536	0.1818	0.0895
	(0.5251)	(0.4734)	(0.4530)	(0.1913)	(0.4950)	(0.1862)
did3	-0.0890	-0.2371	-0.3552	0.2492	0.1226	0.0916
	(0.4382)	(0.4804)	(0.4282)	(0.2130)	(0.5023)	(0.1804)
Insurer FE	N	N	Y	N	N	Y
Year FE	N	N	Y	N	N	Y
Control	N	Y	Y	N	Y	Y
Observations	288	288	288	288	288	288
R^2	0.04909	0.27663	0.77468	0.04003	0.16042	0.87443

Note: This table presents estimates of the impact of the BEAT on the cyber premiums and the market share for the insurers. The continuous treatment (exposure to the BEAT reform) in Panel A is calculated as the share of cyber premiums multiplied by the share of non-US affiliated reinsurance in gross premiums written by the insurer. The treatment group in Panel B is defined as the insurers that have exposure to the BEAT reform above the median. Clustered standard errors at the insurer level are reported in parentheses. ***, **, and * denote the statistical significance at the 1%, 5%, and 10% level, respectively.

Appendix D

This appendix provides detailed information about the reinsurance relationships of insurers, including the intercompany pooling agreement mentioned in Section 4.2. As defined in the main context, the intercompany pooling agreement allows the participants to cede all pooled business to the lead entity and then assume back their stipulated shares from the pool. This provides diversification benefits to the participants by sharing their risks but increases the systematic risk of the group.

This agreement is *de facto* a conventional quota share reinsurance contract, except that the participants are affiliated entities. Therefore, as in normal reinsurance contracts, only the policy-issuing entity has direct liability to its policyholders or claimants, other participants are liable as reinsurers for their share of the issuing entity's obligations. In the accounting process, the direct premiums, losses, and other expenses are recorded as direct businesses, and the proportion ceded to or assumed from the pool is recorded as ceded/assumed reinsurance as typical reinsurance contracts (NAIC, 1998).

Furthermore, the participants of the pooling agreement are not limited to this pooled reinsurance contract. They still have the option of using external reinsurance or other types of reinsurance within the insurance group. The order of pooled reinsurance and other types of reinsurance is not fixed. For example, external reinsurance can be transacted prior to pooling, which means the participants first cede their premiums to third parties and then transfer the rest of their premiums to the pool. Alternatively, the participants could cede premiums to third parties after they assume their shares from the pool. The latter approach is common for the lead insurers in the agreement.

In our data, we can identify the participants of the intercompany pooling agreement by the rating group categorization in AM Best. To estimate the reliance of the rating unit on foreign-affiliated reinsurance, we use the following calculation in Section 6.3:

$$\frac{R_F}{GPW - R_D},$$

where GPW is the gross premiums written of all lines by the rating unit, R_F is the premiums ceded to non-US affiliates, and R_D is the premiums ceded to US affiliates. The reason we use the difference between GPW and R_D in the denominator is that the premiums ceded to the pool are counted twice in the measure of gross premiums. More specifically, the direct underwriting premiums of the participants are first counted as the direct business in their gross premiums and then counted as the assumed business in their lead insurer's gross premiums. Although we do not have information about the order of different types of reinsurance, this does not affect our estimation as we focus on the aggregate premium allocations. However, this measure might underestimate the reliance on foreign-affiliated reinsurance because theoretically, the participants of the pooling agreement may transfer part of their premiums to third parties outside their rating unit (insurers in Bermuda, for example) and then to foreign affiliates.