Journal of Banking and Finance 181 (2025) 107564

Contents lists available at ScienceDirect

Journal of Banking and Finance

journal homepage: www.elsevier.com/locate/jbf

Cyber insurance valuation with endogenous cyber loss

Chang-Chih Chen[a], Chia-Chien Chang[b], Ying Rui[c], Min-Teh Yu[d,*]

[a] Associate Professor of Finance, Providence University, Taiwan
[b] Professor of Finance and Information, National Kaohsiung University of Science and Technology, Taiwan
[c] Doctoral Student in Finance, National Taiwan University, Taiwan
[d] Professor of Quantitative Finance, National Tsing Hua University, Taiwan

ARTICLE INFO

JEL classification:
G22
G13
G32

Keywords:
Cyber risk
Virus attack
Data breach
Cyber loss
Cyber insurance premium

ABSTRACT

This research proposes a novel firm-based model for pricing cyber insurance. Our model considers two types of cyber risk: virus attacks and data breaches. Virus attacks deliver adverse shocks to the firm's productivity, while data breaches cause premium customer departures that worsen the prospect of the firm's product demand. We derive the endogenous structural form of cyber losses in firms and utilize it to solve the formula for cyber insurance premiums. Our quantitative results show that the consensus prediction about a strictly positive premium-risk nexus is no longer valid. Asymmetries in the sub-premium's sensitivity to cyber risks from different sources and the premium customer loss rates jointly shape the complexity of the relation between cyber insurance premiums and cyber risks. Improvements in the product demand conditions enhance firms' incentives to hedge cyber losses and push premiums higher. Lastly, we discuss the influence of product price competition on premiums.

1. Introduction

The rapid digitization of business activities (e.g., financial technology (fintech) and artificial intelligence (AI)) brings forth important issues to both academia and practitioners on how companies manage cyber attacks and effectively hedge against related economic losses.[1,2] One solution to these problems is to buy cyber insurance, as evidenced by over 600 cyber insurance policy forms being offered globally by nearly 100 insurers. In fact, global cyber insurance premiums soared from less than $1 billion in 2012 to $14 billion at year-end 2023, and are likely to grow by 25%-30% per year to reach about $29 billion by 2027.[3] While cyber insurance markets are expanding rapidly and call for immediate attention from academics, progress in cyber insurance research remains limited. Falco et al. (2019) argue that existing cyber insurance valuation largely relies on heuristic estimations of loss severity and frequency. Braun et al. (2023) believe that the lack of better cyber modeling may impede the development of cyber insurance-linked securities markets. As such, the methodologies of insurance valuation must be empirically grounded in science for pricing cyber risk accurately.

One big challenge faced by existing studies lies in the measurement of firms' losses caused by cyber incidents. In the existing models of cyber insurance valuation (e.g., Herath and Herath, 2011; Fahrenwaldt et al., 2018; and Xu and Hua, 2019), cyber losses typically take an arbitrarily designed form or are specified as an exogenous stochastic process unrelated to firm characteristics. Therefore, many unique unobservable

* Corresponding author.
E-mail addresses: bra19810910@yahoo.com.tw (C.-C. Chen), cchiac@nkust.edu.tw (C.-C. Chang), d13723005@ntu.edu.tw (Y. Rui), mtyu@mx.nthu.edu.tw (M.-T. Yu).

[1] Cyber risk typically arises from virus disasters, hacker attacks, or data breaches. Many attempts have been made to define cyber risk; e.g., Eling and Schnell (2016), Eling and Wirfs (2019), and others. Some of them employ a narrow concept that treats cyber risk as the risk involved from electronic events leading to business interruption and monetary loss (Mukhopadhyay et al., 2005, 2013). Others consider a broader perspective by interpreting cyber risk as information security risk or risk that invites failure of information systems (such as Böhme and Kataria, 2006).

[2] Several reports estimate that aggregate economic losses attributed to data breaches could exceed $100 billion. According to a report by Symantec (2013), around $113 billion in losses were attributable to cybercrime in 2012. Estimated cyber losses from McAfee (2014), which include indirect costs such as business interruptions and loss of customers, range from $375 to $575 billion. The survey from Ponemon Institute in 2016 indicates that firms suffer an average loss of $4 million per data breach. For more detailed discussions about the estimate of economic losses due to cyber threats, see Wang (2019).

[3] These numbers are sourced from Global Cyber Risk & Insurance Survey presented by Munich RE in 2024 and S&P Global Survey.

https://doi.org/10.1016/j.jbankfin.2025.107564
Received 4 January 2024; Accepted 30 September 2025
Available online 9 October 2025

parameters are imposed upon models that may pose serious difficulties in calibrating model parameters from conventional empirical data and also make model predictions about cyber insurance premiums less reliable. Moreover, existing cyber insurance pricing models remain silent on how differences in cyber risk sources influence cyber loss formation. Cyber losses from different sources possibly display asymmetric reactions to economic factor changes. Ignoring such reactive asymmetries causes the results of cyber insurance comparative statics to be incomplete, therefore motivating this paper to tackle the aforementioned challenges in cyber insurance valuation.

We propose a firm-based framework for quantifying cyber loss and for pricing cyber insurance. The proposed model allows for two types of cyber risk. Type-I cyber risk refers to the production-side risk arising from virus attacks, which cause brief manufacturing business interruption that partly attenuates the firm's productivity. Type-II cyber risk refers to the sales-side risk triggered by data breaches, which damage the firm's reputation as well as customer trust and further induce premium customer departures. To distinguish between these two types of cyber risk effects, we consider two different channels through which cyber risks affect firm value. The former risk leads to a decrease in instantaneous operating income by damaging production technology, while the latter causes a long-term detrimental effect on the prospect of operating income through premium customer departures. These departures shrink the group of clients from which the firm collects utilizable consumer data, and also weaken the beneficial effect of premium customers on product demand conditions. Our idea for dealing with cyber risks is inspired by Biener et al. (2015), which mention that cyber risk refers to a multitude of different sources of risk affecting a firm's information and technology assets.

In the model, we specify the consequence of type-I cyber risk for a firm as a downward jump in production technology, for which the size of the downward jump depends on the gravity of a virus attack. This gravity can be thought of as the percentage of the firm's computers infected by a virus, and its randomness obeys a truncated normal distribution over the interval from 0 to 1. We model the consequence of type-II cyber risk as structural changes in the product demand dynamics faced by the firm. Data breaches cause the firm to lose a portion of premium customers who purchase its product at a high frequency and in large volumes. Premium customer departures lead to a downward jump in the price sensitivity of the customer base, product demand volatility, and the growth rate of product demand, simultaneously.[4][5] The frequency of cyber incidents obeys a homogeneous Poisson process governed by a time-independent intensity rate.

Given the risk specifications mentioned above, the proposed model allows us to endogenously solve the structural form of a firm's cyber-related *monetary* loss. This form is jointly determined by the firm's product demand and production technology. A key intuition is that we convert intangible customer and technology losses into tangible losses in operating income flows via the firm's product pricing (because the product pricing strategy is a joint function of production technology and product demand). Such a unique model feature enables us to calibrate parameters involved with firms' cyber losses from easily accessible accounting data (e.g., financial statements). Conceptually, we calculate type-I cyber losses as the instantaneous operating income losses from brief manufacturing business interruption. Type-II cyber losses are measured by assessing the influence of deteriorations in the operating income prospect due to premium customer loss (as a consequence of data breaches and of the firm's reputational damage) on firm value. These are two of the most conventional types of losses covered by cyber insurance policies in reality; e.g., Zurich Cyber Insurance Policy, AXA CyberRisk -Connect Product, etc. Using the structural forms of cyber losses, we further derive the analytical formula for cyber insurance premiums. The **total** cyber insurance premium equals the sum of **type-I sub-premium** (for type-I cyber loss) and **type-II sub-premium** (for type-II cyber loss). Our formula facilitates the implementation of numerical analysis (for a summary of model concept, see Fig. 1).

Two insurance pricing implications emerge from our analysis. First, allowing for differences in cyber risk sources is crucial for examining the influence of cyber risk on cyber insurance valuation.

Moreover, the direction of this influence will be reversed by changes in the premium customer loss rate (used as a proxy for the degree of premium customers' aversion to data breaches). When this loss rate is low (high), the total cyber insurance premiums increase with type-I (type-II) cyber risk whereas decrease with type-II (type-I) cyber risk. These outcomes arise from a fact that cyber insurance sub-premiums exhibit asymmetric sensitivities to cyber risks. The magnitude of the influence of changes in the premium customer loss rate on these sensitivities is asymmetric as well.

Although the arrivals of virus attacks and data breaches are mutually independent in the model, increasing the intensity of the type-II (type-I) cyber risk delivers not only a direct positive effect on type-II (type-I) sub-premiums, but also an indirect negative effect on type-I (type-II) sub-premiums. Firms experiencing negative shocks to productivity induced by virus attacks earn fewer profits from premium customers. The fair compensation for losses in premium customer departures due to data breaches is thus lower when the arrivals of virus attacks are more frequent. The negative influence of type-II cyber risk on type-I sub-premium is attributed to the fact that premium customer departures lower the growth rate of product demand and weaken product price competition faced by the firm. Expected operating income losses due to productivity shocks become less when the product demand growth rate is lower. Besides, weak price competition is favorable to the firm suffering virus attacks, because adverse shocks to productivity make the firm raise the product price and such a rise in price discourages few customers when price competition is low (this implies a weak negative impact of virus attacks on operating income). As a result, increasing the frequency of data breaches reduces the fair compensation for expected operating income losses due to virus attacks. The complexities of the relations between cyber insurance premiums and cyber risks are summarized in Fig. 2 for clarity.

The second set of model implications relates to the product market. We find that improvements in product demand conditions enhance firms' incentives to hedge cyber losses, enabling insurers to charge a higher premium for cyber insurance. Such a premium is higher when product demand is larger in size, grows faster, and is less volatile. Notably, the relation between premium and product price competition is complex, depending on the level of the premium customer loss rate.

Price competition in fact influences total premium in two ways. First, it enhances the negative impact of productivity shocks caused by virus attacks on operating income flows. This enhancement effect generates a positive relation between price competition and type-I sub-premium. Second, the patronage of premium customers improves product demand conditions, and therefore, firms absorb the benefits from premium customers by raising product prices (optimal product price is increasing in product demand). This means that, as price competition rises, the available benefits from premium customers reduce and operating income losses due to premium customer departures caused by data breaches fall. Type-II sub-premium thus negatively relates to price

[4] Our assumption of the influence of premium customer departures on the product demand dynamics can be justified using related empirical findings in Gupta and Lehmann (2003), Gupta et al. (2004), Low et al. (2013), Kamiya et al. (2021), Chen et al. (2022), and others. For detailed discussions about assumption justification, please see the last paragraph of Subsection 3C.

[5] We build our cyber-risk specifications upon economic insights from empirical studies. For example, Dynes et al. (2007), Wagner and Bode (2008), and Kelic et al. (2013) find that cyber incidents due to a computer virus disrupt the operations of production infrastructure and information sharing/communications among vertically -related firms. This implies a detrimental influence of virus attacks on productivity. Evidence on customer loss attributed to data breaches has been documented in Garrison and Ncube (2011) and Janakiraman et al. (2018).

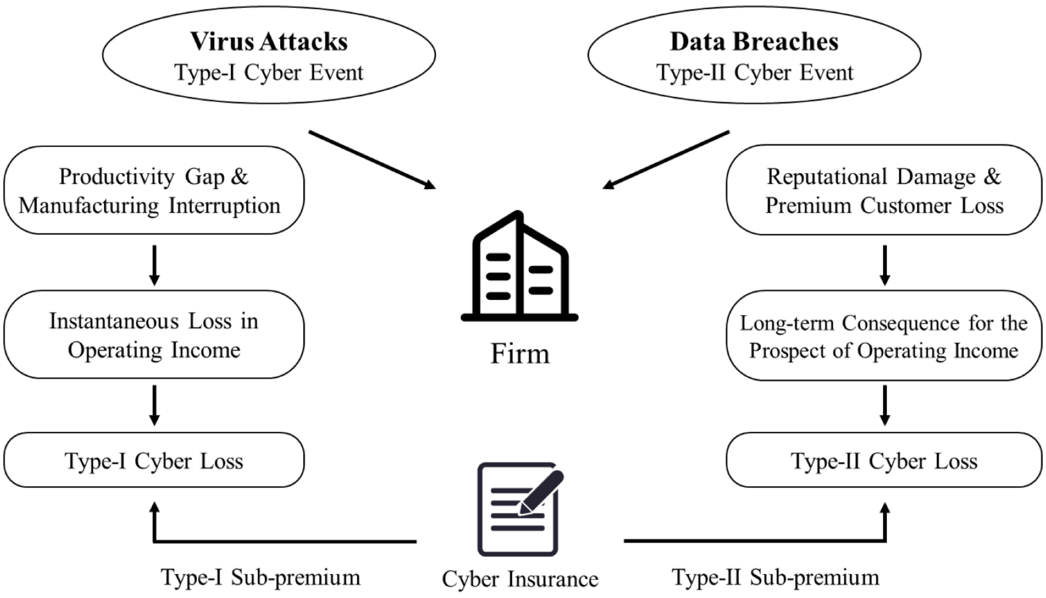
Virus Attacks
Type-I Cyber Event
Data Breaches
Type-II Cyber Event
Productivity Gap & Manufacturing Interruption
Reputational Damage & Premium Customer Loss
Firm
Instantaneous Loss in Operating Income
Long-term Consequence for the Prospect of Operating Income
Type-I Cyber Loss
Type-II Cyber Loss
Type-I Sub-premium
Cyber Insurance
Type-II Sub-premium

Fig. 1. Concept of the firm-based modelling framework.

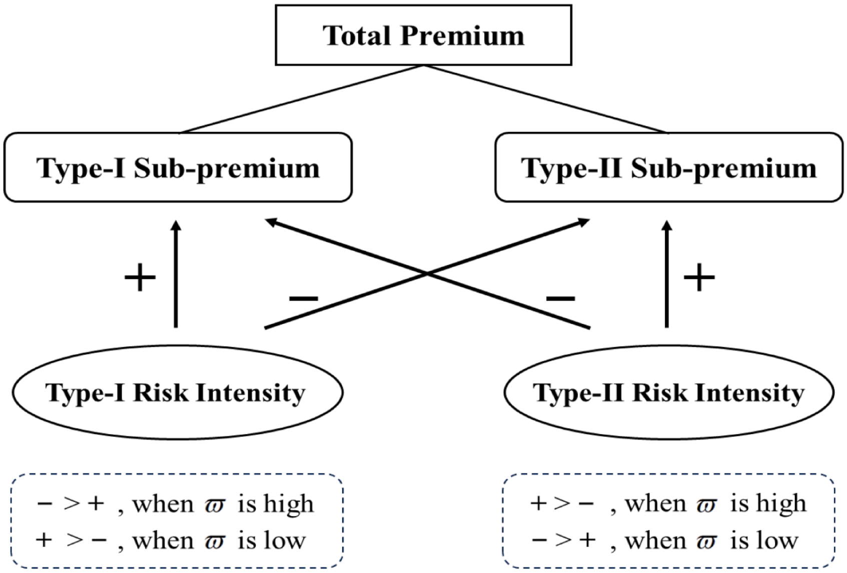

Fig. 2. Impact of cyber risks on cyber insurance premiums. The figure summarizes the complex relationship between cyber risks and cyber insurance premiums. The total premium equals the sum of type-I sub-premium and type-II sub-premium. An increase in type-I (type-II) cyber risk intensity generates a direct positive impact on type-I (type-II) sub-premium and an indirect negative impact on type-II (type-I) sub-premium, simultaneously. When the premium customer loss rate ϖ remains low, the type-I direct impact (type-II indirect impact) dominates, resulting in a positive (negative) relation between the total premium and type-I (type-II) cyber risk. Varying this loss rate from low to high reverses the relations above and associated directions.

competition. When the premium customer loss rate is low (high), the positive (negative) effect of competition on type-I (type-II) sub -premium dominates, so that total premium increases (decreases) with price competition.

The rest of the paper is organized as follows. Section 2 reviews the related literature and presents our research contributions. Section 3 develops the model of cyber loss. Section 4 solves the pricing formula for cyber insurance. Section 5 implements parameter calibration on the basis of a case study. Section 6 discusses quantitative results. Section 7 concludes.

2. Literature review and research contributions

Our paper relates to at least two streams of the literature. The first stream our paper relates to is the theoretical literature on cyber risk and related risk management. Our paper contributes a novel firm-based approach for quantifying cyber loss and pricing cyber insurance. Studies like Gordon et al. (2003) use a descriptive framework to discuss strategies for developing cyber insurance markets, but they never specify how to analyze cyber risk and related economic losses quantitatively. Several subsequent papers make attempts to develop methodologies for gauging cyber risk. Mukhopadhyay et al. (2005) offer a parsimonious utility-based model by treating a cyber-related loss as a disutility. In their numerical examples, the impacts of cyber losses on utility are exogenously pre-determined. Böhme and Kataria (2006) assume that the number of a firm's computers infected by virus attacks obeys a beta-binomial distribution and design cyber losses as a linear function of this number.

In order to study firms' incentives to purchase cyber insurance, Mukhopadhyay et al. (2013) develop a cyber vulnerability assessment model, which has achieved great success in capturing the correlations of cyber incidents among networked organizations, but places less effort at measuring cyber losses. Cyber losses are simply modeled as a binomial random variable. Eling and Jung (2018), Eling and Wirfs (2019), and Eling and Schnell (2020) model them as a stochastic sum (an exogenous compound process). Their models treat loss severity as an independent and identically distributed random variable and further estimate parameters involving the distribution of loss severity by using goodness-of-fit tests. Such an estimation strategy is efficient for macro-level and industry-level risk analyses, but might be unfeasible for firm-level analysis, because the adoption of such an estimation strategy usually requires large-scale cyber loss datasets, and the problems of firm-level data scarcity are still insoluble. Another restriction on the models of these three papers is that they are incapable of examining how an individual firm's behavior and how the difference in cyber risk sources affect cyber loss formation. Similarly, Chong et al. (2023) model cyber losses as a random variable in their tensor-based loss framework for cyber risk assessment. They consider heavy-tailed loss distributions (including Log-Normal, Weibull, and Pareto) and estimate parameters involving the models of loss distributions by fitting industry-wide cyber loss data.

Other studies on cyber risk measurement adopt a copula-based or a network-based approach. Herath and Herath (2007, 2011) and Su et al. (2021) identify cyber risk factors (such as cyberattack frequency or server downtime hours) by using ICSA survey data and then arbitrarily design cyber loss as a joint function of cyber risk factors. They further identify the joint probabilistic distribution of risk factors through copulas and statistical goodness-of-fit tests. Their cyber loss predictions are implemented on the basis of this risk-factor joint distribution. Fahrenwaldt et al. (2018) and Xu and Hua (2019) merge firms' cyber losses, specified as an exogenous stochastic process, into a network model that captures the evolution dynamics of cyber shock contagion among firms. The parameters involving cyber-loss stochastic dynamics (such as information loss volatility) are mostly difficult to estimate or calibrate from observable real data. Such model features hinder subsequent works on the empirical verification for cyber-loss theoretical predictions as well as accuracy assessment.

Overall, existing studies rely on heuristic approaches in which cyber losses take an arbitrarily designed form, evolve according to an exogenous stochastic process, or are specified as a random variable. In contrast, our model offers endogenous structural formulae for quantifying cyber losses solved from the specifications of firm value and operating income. These structural formulae consist of conventional macroeconomic variables and firm characteristic parameters. Hence, it is convenient for us to develop firm-level parameter calibration/estimation strategies by using easily accessible accounting information (e.g., financial statements) and financial market data. On the basis of a case study, we succeed in implementing individual-firm parameter calibration/estimation, which enables us to achieve reliable predictions about firm-level cyber losses and to capture the implication of firm characteristics for cyber loss assessment. Our implementation inspires subsequent studies to execute firm-by-firm cyber loss predictions by following the proposed calibration/estimation strategies.

In addition to convenience in parameter calibration, our model has two other advantages. First, it gives a deeper understanding of the comparative statics of cyber insurance premiums. Our model decomposes the total premium into type-I sub-premium and type-II sub-premium. Such a premium sub-categorization permits us to identify through which channels changes in economic factors affect the total premiums and to examine asymmetries in the responses of cyber losses from different risk sources to these changes. Second, our model captures the implications of product market dynamics and across-firm differences in product-demand-specific factors (e.g., product demand growth rate, volatility, and size) for cyber insurance valuation. These implications elucidate the relevance of the product market's permanent fluctuations in assessing firms' cyber losses and further offer insurance market participants a new and useful guide to determine reasonable cyber insurance premiums. To better highlight our model advantages, we present a detailed comparison among our model and the aforementioned cyber risk models in Appendix A.

The second stream our paper relates to is the literature on insurance valuation. Many attempts have been made to propose valuation theories for various insurance products: e.g., deposit insurance (Duan and Yu, 1999), life insurance (Fischer, 2007; Young, 2008; Chen et al., 2022), health insurance (Baione and Levantesi, 2014; Yang et al., 2016), catastrophe insurance (Lee and Yu, 2007; Chang et al. 2011), unemployment insurance (Chuang and Yu, 2010; Biagini et al., 2013), insurance guaranty (Duan and Yu, 2005), mortgage insurance (Chang et al., 2012; Chen and Chang, 2019), etc. To our knowledge, however, little attention is paid to cyber insurance valuation. We fill the gap in this line of research by proposing a novel firm-based cyber risk model for pricing cyber insurance. The model allows us to derive an analytical formula for cyber insurance premiums, which is tractable for doing numerical computation as well as large-scale comparative statics analysis. The model results indicate that, in addition to cyber risk factors, the inclusion of product market conditions faced by firms is a must for determining cyber insurance premiums that can provide insurance companies forward- looking guidance for formulating customized premium schemes for specific firms.

3. A firm-based model of endogenous cyber loss

Consider a continuously trading economy supported by a probability space $(\Omega, \mathscr{F}, (\mathscr{F}_t)_{t\geq 0}, \mathbb{Q})$ satisfying the usual conditions. The economy consists of totally-equity-financed firms and insurance companies. The firms engage in producing and selling output, while the insurance companies engage in selling term insurance contracts against firms' losses in cyber events. The insurance markets are perfectly competitive and frictionless.

3.1. Production function

As in Miao (2005), the representative firm rents capital at the rental rate $\delta > 0$ to produce output with the production function: $F : \mathbb{R}_+ \to \mathbb{R}_+$, $F(k(t)) \equiv (k(t))^{\gamma}$, where $\gamma \in (0,1)$ is the return-to-scale parameter, and $k(t)$ is the amount of capital input at time *t*.

3.2. Type-I cyber event and its consequences for production technology

The number of occurrences of type-I cyber events is counted by a Poisson process with time- independent instantaneous intensity λ_I, similar to Herath and Herath (2007, 2011) and Su et al. (2021). The density function of the random time of the i^{th} type-I cyber event $\widetilde{T}_i$ thus takes the form $\tilde{f}_i(t) = \lambda_I e^{-\lambda_I t}(\lambda_I t)^{i-1}[(i-1)!]^{-1}$. The arrival of a cyber event creates a sudden shock to the firm's production technology (for evidence of the impact of virus attacks on productivity, see Kelic et al., 2013). Given this fact, we specify production technology as $A(t) = \boldsymbol{A} - \sum_{i=1}^{\infty} 1_{(t=\tilde{T}_i)} x_i \boldsymbol{A}$, where $\boldsymbol{A}$ is the permanent time-independent level of production technology and x_i denotes the gravity of the i^{th} virus attack shock. This gravity reflects the percentage of a firm's computers infected by the i^{th} virus. Its role is to determine the magnitude of a virus-attack shock to the firm's productivity. As the gravity increases, the firm's productivity reduces proportionally. In the extreme case where the gravity reaches 100% (all of the firm's computers are infected $x_i \to 100\%$), the virus attack damages electronic systems outright, and causes a complete interruption of manufacturing operation, which implies $A(\tilde{T}_i) \to 0$ (the firm's productivity drops to zero).[6]

The firm regains its original technology and recovers from virus attacks by rehabilitating its electronic production systems, but the recovery incurs a gravity-dependent cost taking a generalized form of $C(x_1, x_2, \cdots) = \sum_{i=1}^{\infty} 1_{(t=\tilde{T}_i)} x_i \boldsymbol{c}$.[7] In this linear cost specification, $\boldsymbol{c}$ represents the cost for rehabilitating the firm's entire electronic production systems.[8] This specification captures the positive sensitivity of recovery cost to the gravity of virus attacks. The firm experiencing a higher-gravity virus attack incurs greater costs in restoring its electronic production systems. Specifically, the recovery cost for each type-I cyber event reaches $\boldsymbol{c}$ if the virus attack causes an outright failure of the electronic systems, effectively halting the entire manufacturing business ($x_i \to 100\%$).

Without loss of generality, we assume $(x_i)_{i=1}^{\infty}$ to be independent and identically-distributed (*iid.*) random variables obeying a truncated normal distribution defined over [0,1]. The probability density function of x_i with mean $\mu_x(\alpha,\beta)$ and variance $\sigma_x^2(\beta)$ is given below:

$$f_x(x) = \beta^{-1} \mathrm{n}\left[(x-\alpha)\beta^{-1}\right]\left\{\mathrm{N}\left[(1-\alpha)\beta^{-1}\right] - \mathrm{N}\left[-\alpha\beta^{-1}\right]\right\}^{-1},$$

where (α, β) are constants, $\mathrm{n}[\cdot]$ denotes the density function of a standard normal distribution and $\mathrm{N}[\cdot]$ denotes the corresponding cumulative probability function.

3.3. Type-II cyber event and its consequences for product demand

Similar to type-I cyber events, the number of occurrences of type-II cyber events is counted by a Poisson process with time-independent instantaneous intensity λ_{II}. The occurrences of these two types of cyber events are independent of each other. The random time of the i^{th} type-II cyber event $\overline{T}_i$ thus has a density function that takes the form of $\overline{f}_i(t) = \lambda_{II} e^{-\lambda_{II} t}(\lambda_{II} t)^{i-1}[(i-1)!]^{-1}$. The arrival of a type-II cyber event, which usually entails data breaches, damages the firm's reputation and erodes customer trust. Hence, as demonstrated by Janakiraman et al. (2018), the outbreak of data breaches further causes the firm to lose a portion of premium customers through reputational damage. Compared to normal customers, premium customers purchase the firm's product more frequently and in larger volumes. Premium customers' patronage improves sales/earnings growth but amplifies corresponding fluctuations. Besides, premium customers exhibit a higher price sensitivity due to (i) the greater influence of price changes on their wealth; and (ii) their access to abundant reference- price information, which makes them more responsive to price adjustments. Premium customers' departures result in a simultaneous decline in the firm's aggregate product demand volatility, product demand growth rate, and the price elasticity of the customer base.

Given the facts above, we thus express the firm's aggregate product demand as:

$$\widehat{Q}_D(p(t), Q_d(t)) \equiv q(p(t))Q_d(t) \equiv p(t)^{-\varepsilon(t)}Q_d(t)$$

where $p(t)$ is the product price chosen by the firm at time t, $q(\cdot)$ is the size of the customer base, $(\varepsilon(t))_{t\geq 0} \in (1, 1+\gamma^{-1})$ is the customer-to-price elasticity, and $Q_d(t)$ is the average demand per customer, governed by a Brownian motion $B(\cdot)$.[9] Specifically, the average product demand evolves according to $dQ_d(t)/Q_d(t) = \mu(t)dt + \sigma(t)dB(t)$, where $\mu(t)$ denotes the expected growth rate, $\sigma(t)$ denotes the volatility rate, and $Q_d(0) \equiv \boldsymbol{Q}$ is initial product demand.

We next specify the three parameters that capture the effect of premium customer departures (denoted by ϖ) on product demand and the customer-price elasticity:

$$\sigma(t) = \sigma_L + (\sigma_U - \sigma_L)\prod_{i=1}^{\infty}\left(1 - \varpi 1_{(\overline{T}_i \leq t)}\right); \mu(t) = \mu_L + (\mu_U - \mu_L)\prod_{i=1}^{\infty}\left(1 - \varpi 1_{(\overline{T}_i \leq t)}\right),$$
$$\varepsilon(t) = \varepsilon_L + (\varepsilon_U - \varepsilon_L)\prod_{i=1}^{\infty}\left(1 - \varpi 1_{(T_i \leq t)}\right).$$

In the above specifications, σ_U, μ_U, and ε_U (σ_L, μ_L, and ε_L) denote the upper (lower) bounds of parameter values. The second terms on the right-hand side of these three specifications capture increments in product demand volatility, product demand growth, and the customer-to-price elasticity created by premium customers. These imply that, as the number of occurrences of type-II cyber event increases, premium customer departures make (i) the firm's product demand become less volatile, (ii) product demand grow at a slower pace, and (iii) the size of the customer base dis- play a weaker sensitivity to product price adjustments. The marginal effect of premium customer departures on the prospect of product demand as well as price elasticity gradually decreases with the number of cyber event occurrences (because for $t \to \overline{T}_i$, $\mathbb{E}_0^{\mathbb{Q}}\varepsilon(\overline{T}_i) = \varepsilon_L + (\varepsilon_U - \varepsilon_L)(1-\varpi)^i$, $\mathbb{E}_0^{\mathbb{Q}}\sigma(\overline{T}_i) = \sigma_L + (\sigma_U - \sigma_L)(1-\varpi)^i$, and $\mathbb{E}_0^{\mathbb{Q}}\mu(\overline{T}_i) = \mu_L + (\mu_U - \mu_L)(1-\varpi)^i$). The convexity of this effect suggests

[6] The productivity gap due to virus attack $A - A(1-x_i)$ has a positive linear relation with virus-attack gravity. To capture the convexity/concavity of this relation, one can consider $A(t) = A - \sum_{i=1}^{\infty} 1_{(t=\tilde{T}_i)} x_i^{\nu} A$ where ν is a positive constant. Marginal changes in the productivity gap due to a rise in the gravity decrease (increase) with gravity, and the productivity gap is concave (convex) in gravity, if $0 < \nu < 1$ $(1 < \nu)$. We find no empirical evidence to determine the shape of the impact of virus attacks on the productivity gaps. Given this uncertainty, we adopt a parsimonious production technology specification that fixes a negative linear relationship between productivity technology and virus attacks. This linearity means that the productivity gap widens at a constant rate as the gravity of virus attacks increases, providing a straightforward and intuitive approach for the model.

[7] The inclusion of random recovery time would add complexity to the model without generating additional economic insights into the associations among cyber risks, cyber losses, and cyber insurance premiums. Our main results remain unchanged after taking the randomness of recovery time into account. Our assumption on prompt recovery in fact aligns with the circumstances of most companies. For example, a cyber security survey commissioned by the U. K. government in 2023 shows that the vast majority of businesses (88%) and charities (84%) are able to restore operations within 24 hours after suffering a disruptive cyber attack. Approximately 70% of these organizations indicate almost immediate recover following cyber attacks. Similar findings are available in the 2001-2004 ICSA (International Computer Security Association) virus reports. The assumption of prompt recovery thus does not hinder our ability to measure firms' losses from type-I cyber attacks.

[8] We can easily extend our model by allowing for the convexity/concavity of recovery costs with respect to the gravity of virus attacks. Taking the case of the i^{th} attack as an example, the recovery cost can be expressed as $1(t = \tilde{T}i)x_i^{\theta}c$ where θ determines the shape of the gravity sensitivity of recovery costs. This shape is convex (concave) when $\theta > 1$ $(1 > \theta > 0)$. To the best of our knowledge, no empirical evidence clarifies whether this shape is convex or concave. Hence, we adopt the linear cost specification for simplicity and clarity.

[9] We impose finite bounds on price elasticity in order to ensure the existence of an optimal product price.

that a premium customer with larger purchase volumes or a higher purchase frequency is more likely to depart earlier. Such an early departure causes more significant damage to the firm's sales performance. This is because a customer's exposure to data breach risk increases with his purchase volumes/frequency. Greater risk exposure motivates such a customer to suspend his patronage or migrate to other unbreached firms sooner. The marginal effect of premium customer departures eventually disappears as the number of data breach occurrences approaches infinity. This reflects the cumulative impact of relentless data breaches, which erodes customer trust and ultimately results in the loss of all premium customers, thereby severing their patronage with the firm.

Our specifications of product demand dynamics and customers' price elasticity can be justified via several related empirical findings. Gupta and Lehmann (2003) and Gupta et al. (2004) find that the expected value created by customers is more significant when the customer growth rate is higher, which implies a higher product demand growth rate. Premium customer departures reduce the total expected value of customers, so that such departures are associated with a decrease in the product demand growth rate. Kamiya et al. (2021) document that cyberattacks lead to a consequent decrease in sales growth for both large firms and retail firms. Firms respond to cyberattacks by attenuating managerial risk-taking incentives. Chen et al. (2022) find that CEO risk taking increases with the level of customer concentration. Also, Cao et al. (2023) hold that customer concentration enhances major customers' bargaining power, forcing firms to take on higher business risks by maintaining high levels of inventories and receivables. These findings imply an inverse association between firm risk and premium customer departures, because data breaches lower the firm's reliance on premium customers, thereby altering its risk profile. Kalyanaram and Winer (1995) argue that high-patronage customers possess abundant reference-price information and often refer to past prices when making purchase decisions. Chang and Wildt (1994) and Low et al. (2013) further demonstrate that reference prices affect customers' perception of product value and market pricing. High-patronage customers thus have a deeper understanding of market price conditions, making them more sensitive to price differences. These arguments align with our assumption that premium customer loss attenuates the price elasticity of the customer base.

3.4. Cyber insurance contract

Consider an insurance company that sells term insurance contracts against firms' losses caused by cyber incidents. These contracts do not cover third-party-related indirect losses; e.g., fraudulent electronic transfers or damage to customers' reputations. Because our primary research interest lies in the measurement of a firm's cyber losses (first-party direct losses), the coverage for third-party indirect cyber losses is beyond the scope of our research.[10]

The contract expires at date T, promises to cover a portion ϕ of the insured's operating income loss in cyber incidents, and is equipped with deductibles and coverage upper limits. Both they are defined on the gravity of virus attacks and the number of cyber event occurrences.[11] Specifically, we consider the knock-in lower and knock-out upper barriers for gravity and the number of cyber events, including (x_U, x_L), $(\widetilde{U}, \widetilde{L})$, and $(\overline{U}, \overline{L})$. The insured receives compensation for cyber losses only if (i) the number of cyber event occurrences is equal to or larger than $(\widetilde{L}, \overline{L})$ but less than $(\widetilde{U}, \overline{U})$ and (ii) the gravity of a virus attack falls within the range from x_L to x_U. Hence, the three knock-out barriers and knock-in barriers respectively capture the implications of coverage limits and of deductibles.

The fair cyber insurance total premium $I(\cdot)$ solves the following pricing equation:

$$\begin{aligned} I(0) &= \sum_{i=\tilde{L}}^{\tilde{U}-1} \mathbb{E}_0^Q \phi \widetilde{L}(\widetilde{T}_i) e^{-r\tilde{T}_i} 1_{(\tilde{T}_i \le T)} 1_{(x_L \le x_i \le x_U)} + \sum_{i=\overline{L}}^{\overline{U}-1} \mathbb{E}_0^Q \phi \overline{L}(\overline{T}_i) e^{-r\overline{T}_i} 1_{(\overline{T}_i \le T)} \\ &\equiv \widetilde{I}(0) + \overline{I}(0), \end{aligned} \tag{1}$$

where r is the subjective discount rate and the contractual parameters satisfy the usual conditions: $0 \le x_L < x_U \le 1$, $1 \le \widetilde{L} < \widetilde{U}$, and $1 \le \overline{L} < \overline{U}$. In the pricing equation, $\widetilde{L}(\cdot)$ and $\overline{L}(\cdot)$ represent the insured's loss due to i^{th} type-I and i^{th} type-II cyber events, respectively. As mentioned in Sections 3.B-3.C, $\widetilde{L}(\cdot)$ is equivalent to the recovery cost plus instantaneous operating income loss caused by the productivity gap arising from brief manufacturing business interruption, while $\overline{L}(\cdot)$ can be treated as long-term operating income loss (since the prospect of operating income deteriorates) due to premium customer departures invited by the firm's reputational damage as a consequence of data breaches. These are two of the most conventional types of losses covered by cyber insurance policies in practice; e.g., the Zurich Cyber Insurance Policy, the AXA CyberRiskConnect Product, etc.[12]

4. Cyber insurance valuation

We now derive the valuation formula for cyber insurance in two steps. In the first step, we solve for the optimal product price and then merge this optimal pricing strategy into the specification of the firm's operating income. In the second step, we solve for the structural formulae of losses due to cyber incidents using the specification of operating income under optimal product pricing. These structural formulae of cyber losses enable us to calculate the total present value of risk compensation offered by a cyber insurance contract, which helps us determine fair insurance premiums.

4.1. Product pricing strategy and operating income under optimal pricing

We express instantaneous operating income at time t as:

$$\widehat{\pi}(p(t), Q_d(t), A(t)) = \underbrace{p(t)\widehat{Q}_D(p(t), Q_d(t))}_{salesrevenue} - \underbrace{\delta k^*(p(t), Q_d(t), A(t))}_{productioncosts} \tag{2}$$

In (2), the equilibrium input demand $k^*(t) = [p(t)^{-\varepsilon(t)} Q_d(t)/A(t)]^{1/\gamma} \equiv k^*(p(t), Q_d(t), A(t))$ is solved from the market-cleaning condition $\widehat{Q}_D(p(t), Q_d(t)) = \widehat{Q}_S(A(t), k^*(t)) = A(t)F(k^*(t))$. The objective of firm managers is to choose an optimal product price that maximizes instantaneous

[10] Franke (2017) finds that the coverage policy of cyber insurance products issued in the U.S. is historically different from that in Europe. The former primarily focuses on third-party liabilities connected with data and privacy breaches; whereas the latter targets first-party direct costs of business interruption. The contract we consider therefore appears like a "European-style" cyber insurance contract.

[11] Coverage limits and deductibles are both widely-used mechanisms through which insurance companies in reality address potential adverse selection problems. Conceptually, deductibles refer to self-absorption losses borne by the insured before his coverage kicks in, while coverage upper limits impose a cap on the insurer's liability for losses emerging from the insurance policy.

[12] Our insurance coverages align well with those in practice. For example, the policy of AXA CyberRiskCon- nect Product provides coverage for data-breach consequential reputational loss, business interruption loss, and related extra expenses. Similarly, the Zurich Cyber Insurance Policy offers a comprehensive range of coverages; e.g., losses from reputational damage, business income losses due to system failures, and cyberattack extortion expenses. Additionally, the Coalition Active Cyber Insurance has various optional coverages, though coverage for reputational harm losses is available only as an add-on through additional endorsements. Cyber insurance policies so far are more prevalent in North America (accounts for 43% of global cyber insurance market share in 2023) and Europe but less in Asia and other regions.

operating income - that is: $\max_{p(t)>0}\overset{\wedge}{\pi}(p(t),Q_d(t),A(t))$. Its explicit solution is given as follows.

Theorem 1. **(Optimal Product Pricing)** *Given operating income as equation (2), the firm sells its products at* $p^*(t)=Q_d(t)^{(1-\gamma)/\eta(t)}A(t)^{-1/\eta(t)}\left(\frac{\delta\varepsilon(t)}{\varepsilon(t)-\eta(t)}\right)^{\gamma/\eta(t)}$, *where* $\eta(t)\equiv(1-\gamma)\varepsilon(t)+\gamma$. *The optimal price is strictly increasing in product demand* $(\partial p^*(t)/\partial Q_d(t)>0)$ *but strictly decreasing in production technology* $(\partial p^*(t)/\partial A(t)<0)$.

Plugging the optimal product price into the income function (2), we yield the explicit form of instantaneous operating income under optimal product pricing $\widehat{\pi}(p^*(t),Q_d(t),A(t))\equiv\widehat{\pi}^*(t)$:

$$\widehat{\pi}^*(t)\equiv\widehat{\pi}^*(Q_d(t),A(t))=Q_d(t)^{1/\eta(t)}A(t)^{(\varepsilon(t)-1)/\eta(t)}\left(\frac{\delta\varepsilon(t)}{\varepsilon(t)-\eta(t)}\right)^{1-\varepsilon(t)/\eta(t)}\frac{\eta(t)}{\varepsilon(t)} \tag{3}$$

Note that operating income has been converted into a joint function of production technology and product demand. Using (3), we derive the structural formulae for cyber losses below.

4.2. Structural formula for type-I cyber losses

We measure the firm's losses due to the i^{th} occurrence of type-I cyber event by

$$\widetilde{L}(\widetilde{T}_i)=x_i\boldsymbol{c}+\widehat{\pi}^*(Q_d(\widetilde{T}_{i-}),A(\widetilde{T}_{i-}))-\widehat{\pi}^*(Q_d(\widetilde{T}_i),A(\widetilde{T}_i)), \tag{4}$$

which equals the sum of (i) the cost for recovering original production technology and (ii) losses to instantaneous operating income induced by the productivity gap. The adverse shock of the i^{th} virus attack to production technology generates a gap between $\boldsymbol{A}(1-x_i)$ and $\boldsymbol{A}$, which results from brief manufacturing business interruption. The present value of type-I risk compensation is shown below.

Theorem 2. **(Present Value of i^{th} Type-I Cyber Risk Compensation)** *Given (2)-(4),* i^{th} *type-I cyber risk compensation has a present value* $\mathbb{E}_0^{\mathrm{Q}}\phi\widetilde{L}(\widetilde{T}_i)\mathrm{e}^{-r\tilde{T}_i}1_{(\tilde{T}_i\le T)}1_{(x_L\le x_i\le x_U)}=\sum_{j=0}^{\infty}\widetilde{V}(i,j)$ *wheres*

$$\widetilde{V}(i,j)=\begin{cases}\int_0^T\int_t^\infty\int_{x_L}^{x_U}\Phi(j,z,t)\overline{f}_1(t_1)dzdt_1dt, j=0\\ \int_0^T\int_{t_1}^T\int_{t_2}^T\cdots\int_{t_j}^T\int_t^\infty\int_{x_L}^{x_U}\Phi(j,z,t)\prod_{k=1}^{j+1}\overline{f}_k(t_k)dzdt_{j+1}dtdt_j\cdots dt_2dt_1, j=0\end{cases}$$

$$y_i\equiv y_L+\left(y_U-y_L\right)(1-\varpi)^i, y=\sigma,\mu,\varepsilon;\eta_i\equiv\varepsilon_i+\gamma-\gamma\varepsilon_i;$$
$$\Phi(j,z,t)\equiv\varphi(j,z)\mathrm{e}^{-rt}\phi f_x(z)\widetilde{f}_i(t);\varphi(j,z)\equiv\nu(j)-(1-z)^{(\varepsilon_j-1)/\eta_j}\nu(j)+z\boldsymbol{c};$$
$$\nu(j)\equiv\boldsymbol{Q}^{1/\eta_j}\mathrm{e}^{\varsigma(j)}\Xi(\varepsilon_j,\eta_j);\Xi(a,b)\equiv\boldsymbol{A}^{(a-1)/\mathrm{b}}\delta^{1-\mathrm{a}/\mathrm{b}}a^{-a/\mathrm{b}}(a-b)^{a/\mathrm{b}-1}b;$$
$$\varsigma(j)\equiv\xi\left(\eta_j,\mu_j,\sigma_j,t_j,t\right)+1_{(j>0)}\sum_{k=1}^{j}\xi(\eta_j,\mu_{k-1},\sigma_{k-1},t_{k-1},t_k);$$
$$\text{and }\ \xi(l,m,n,u,v)\equiv(v-u)l^{-1}\left(m+0.5n^2\left(l^{-1}-1\right)\right).$$

4.3. Structural formula for type-II cyber losses

We measure the firm's losses in the i^{th} type-II cyber event as $\overline{L}(\overline{T}_i)=\widehat{L}(\overline{T}_{i-})-\widehat{L}(\overline{T}_i)$ where $\widehat{L}(t)\equiv\mathbb{E}_t^{\mathrm{Q}}\int_t^\infty\widehat{\pi}^*(Q_d(s),\boldsymbol{A})\mathrm{e}^{-r(s-t)}ds-\sum_{j=1}^\infty\mathbb{E}_t^{\mathrm{Q}}(\widehat{\pi}^*(\widetilde{T}_{j-})-\widehat{\pi}^*(\widetilde{T}_j))\mathrm{e}^{-r(\tilde{T}_j-t)}1_{(t<\tilde{T}_j)}$. Take the term $\widehat{L}(\overline{T}_{i-})$ as an example for clarification. The first part, $\mathbb{E}_{\overline{T}_{i-}}^{\mathrm{Q}}\int_{\overline{T}_{i-}}^\infty\widehat{\pi}^*(Q_d(s),\boldsymbol{A})\mathrm{e}^{-r(s-T_{i-})}ds$, refers to the total expected value (at time $\overline{T}_{i-}$) of future operating income in the absence of type-I cyber risk. The second part, $-\sum_{j=1}^\infty\mathbb{E}_{\overline{T}_{i-}}^{\mathrm{Q}}(\widehat{\pi}^*(\widetilde{T}_{j-})-\widehat{\pi}^*(\widetilde{T}_j))\mathrm{e}^{-r(\tilde{T}_j-\overline{T}_{i-})}1_{(\overline{T}_{i-}<\tilde{T}_j)}$, refers to the aggregate negative effect of type-I cyber risk on the total expected value of discounted operating income in the future. The sum of these two parts represents the total expected value (at $\overline{T}_{i-}$) of future operating income with allowing for the effects of type-I cyber risk. The negative effect of premium customer departures on such a total expected value thus can be understood as data-breach consequential long -term losses to operating income. This value effect contributes a natural guide to type–II cyber loss measurement. The present value of type-II risk compensation is given below.

Theorem 3. **(Present Value of i^{th} Type-II Cyber Risk Compensation)** *Given* $\overline{L}(\overline{T}_i)$ *and equation (3),* i^{th} *type-II cyber risk compensation has a present value* $\mathbb{E}_0^{\mathrm{Q}}\phi\overline{L}(\overline{T}_i)\mathrm{e}^{-r\overline{T}_i}1_{(\overline{T}_i\le T)}=\overline{V}(i)$ *where*

$$\overline{V}(i)=\begin{cases}\int_0^T(\omega(0,t_{1-},0,1,1)-\omega(1,t_1,0,1,1))\phi\mathrm{e}^{-rt_1}\overline{f}_1(t_1)dt_1, i=1\\ \int_0^T\int_{t_1}^T\cdots\int_{t_{t-1}}^T(\omega(i-1,t_{i-},i-1,1,1)-\omega(i,t_i,0,1,0))\phi\mathrm{e}^{-rt_i}\prod_{n=1}^{i}\overline{f}_n(t_n)dt_i\cdots dt_1, i>1\end{cases}$$

$$\omega(a,b,c,d,e)\equiv\boldsymbol{Q}^{1/\eta_a}\mathrm{e}^{\imath(a,b,c,e)\times d}\Upsilon(\varepsilon_a,\eta_a,\mu_a,\sigma_a,b);$$
$$\imath(u,v,w,x)\equiv x\xi(\eta_u,\mu_w,\sigma_w,t_w,v)+1_{(u>1)}\sum_{k=1}^{u}\xi(\eta_u,\mu_{k-1},\sigma_{k-1},t_{k-1},t_k);$$
$$\Upsilon(a,b,c,d,e)\equiv(r-\xi(b,c,d,0,1))^{-1}\times\Xi(a,b)-\sum_{j=1}^{\infty}\Delta(a,b,c,d,e,j);$$
$$\Delta(a,b,c,d,e,j)=\Xi(a,b)\int_e^\infty\int_0^1\rho(a,b,z)\mathrm{e}^{\xi(b,c,d,e,t)\widetilde{-r(t-e)}}f_x(z)f_j(t,e)dzdt;$$
$$\rho(u,v,w)\equiv1-(1-w)^{(u-1)/v};and\widetilde{f}_i(t,s)=\lambda_I\mathrm{e}^{-\lambda_I(t-s)}(\lambda_I(t-s))^{i-1}[(i-1)!]^{-1}.$$

4.4. Formula for cyber insurance premiums

We are ready to derive the valuation formula for cyber insurance. By using expression (1) and Theorems 2-3, we yield the analytical-form solution to insurance premiums:

$$I(0)=\widetilde{I}(0)+\overline{I}(0)=\sum_{i=\tilde{L}}^{\tilde{U}-1}\sum_{j=0}^{\infty}\widetilde{V}(i,j)+\sum_{i=\overline{L}}^{\overline{U}-1}\overline{V}(i).$$

Note that the total cyber insurance premium includes two parts. The first part $\widetilde{I}(0)$ and the second part $\overline{I}(0)$, respectively, refer to the compensation for type-I cyber events and type-II cyber events. Such a separation allows us to study whether and how cyber losses from different sources exhibit asymmetric responses to changes in economic factors, which we do in the subsequent section.

5. Parameter calibration implementation in a case study[13]

Section 5 implements baseline parameter calibration on the basis of a case study of "The TJX Companies", a U.S. nonfinancial listed company. The selection of TJX is motivated by several factors. First, TJX's business mainly comprises the manufacture and retail of apparel and home fashions, so it operates in a business-to-customer environment that aligns well with our assumption. Second, TJX experienced a serious cyberattack in 2007, which enables us to empirically assess its consequential impact on operating performance and related financial variables (e.g., operating income volatility or growth). Third, TJX offers more comprehensive post-cyberattack accounting information, ensuring the reliability of estimating/calibrating firm-characteristic parameters after a cyberattack. In contrast, other firms provide limited information, mostly less than three firm-year observations.

We collect TJX's accounting data from Compustat and construct a 1960-2019 firm sample with 59 firm-year observations. The parameters are categorized into three groups: (i) cyber event-related parameters, calibrated at the market/country level; (ii) firm characteristic parameters, estimated from TJX's accounting data; and (iii) contractual parameters, normalized at moderate levels. Our model calibration strategies are as follows.

5.1. Cyber event parameters

Consider first the parameters governing type-I cyber events. Data reported by the 2001-2004 ICSA virus survey show that the average ratio of annual virus-attack server downtime total hours to annual hours (365×24) equals 0.208. Accordingly, we choose the intensity of type-I cyber risk λ_I at 20%. This value is close to the estimate from the 2015-2024 Cyber Security Breaches Survey technical reports commissioned by the U.K. government, which indicates that the average percentage of businesses identifying virus attacks within a year reaches 17.75%. We choose the two probabilistic parameters of virus-attack gravity (α,β) at (58.004%, 9.99%), which help us match the mean $\mu_x(\alpha,\beta)$ and standard deviation $\sigma_x(\beta)$ of gravity with 58% and 10%, respectively. These two numbers are borrowed from Statista's 2010 international survey on computer virus infection, which presents an average infection rate of 58% and a standard deviation of 10%. We calibrate the recovery cost parameter $\boldsymbol{c}$ at \$2.837. This makes the ratio of the expected recovery cost to initial operating income $\boldsymbol{c}\mu_x/\widehat{\pi}^*(0)$ match the observed ratio of TJX's 2007 cyber attack losses (data source: EM360 Tech official website) to its operating income in the same year, equaling 17.7072%.

Consider next the parameters governing type-II cyber events. During 2005-2023, the average annual number of data breaches in the U.S. approximates 990 (data source: Statista official website). With approximately 9,000 publicly listed companies in the U.S. (Compustat) during this period, the average annual frequency of data breaches per firm is approximately 0.11008. So, we set the intensity of type-II cyber risk λ_{II} at 11.008%. We set the premium customer loss rate ϖ at 20%, a relatively conservative level. According to PCI Pal's 2019 global research, data breaches significantly affect customer retention. In the U.S. and Canada, over 20% of consumers would never return to a business following a breach, while in Australia and the U.K., this consumer loss rate even exceeds 40%. This highlights the severe reputational and financial consequences firms face post-breach.

5.2. Firm characteristic parameters

Consider first the four firm-characteristic parameters unaffected by cyber events. For brevity, we normalize initial product demand $\boldsymbol{Q}$ to be 10 and permanent production technology $\boldsymbol{A}$ to be 5. Our results only vary quantitatively but not qualitatively with these two parameters. As in Miao (2005), we measure the capital rental rate δ using the sum of the riskless interest rate and capital depreciation rate. The riskless interest rate is chosen at 4.898%, estimated from 1962-2023 one-year treasury bill rate data. The capital depreciation rate is set to be 9.193%, consistent with the average ratio of TJX's depreciation expenses to its PPE (Property, Plant, and Equipment). Following Miao (2005), we borrow the estimation results from Caballero and Engel (1999) and calibrate the return-to-scale parameter γ at 40%.

Consider next the upper bounds of the product demand growth rate, product demand volatility, and price elasticity of customers. These three parameters manifest the outlook for product demand in a data-breach-free scenario. We first calibrate the upper bound of the customer-to-price elasticity ε_U from the formula for the structural relationship among the return-to-scale parameter, the price-elasticity upper bound, and the elasticity of sales revenue to the markup pricing rate (defined as the ratio of sales revenue to production costs) conditional on the data-breach-free scenario ξ_{pre}:[14]

$$\xi_{pre} = \frac{1}{1-\gamma^{-1}+\frac{\gamma^{-1}}{1-\varepsilon_U}} + \frac{2}{1-\gamma^{-1}} \tag{5}$$

In (5), the elasticity of sales revenue is estimated using data on TJX's sales revenue and cost of goods sold (i.e., proxy for production costs) from 1960 to 2006 (pre-data-breach period) and regressing the changes in sales revenue *Sales* on the changes in the markup pricing rate *Markup*:[15]

$$\Delta \ln Sales_t = \xi_{pre}\Delta \ln Markup_t + \vartheta_t \tag{6}$$

where the operator Δ represents the difference between year t and base-year $t-k$ and ϑ_t is the error term. Prior studies (e.g., Doerrenberg et al., 2017; Neisser, 2021; etc.) typically consider 1-year or 2-year differences. Accordingly, we take the average of estimates given $k=1$ and $k=2$, which shows $\xi_{pre} = -1.467$. Using this number and formula (5) given $\gamma = 40\%$ yields the implied level of the upper bound of price elasticity $\varepsilon_U = 1.417$. We calibrate the upper bounds of the product demand growth rate μ_U and of volatility σ_U at 29.473% and 49.943%, respectively. These two numbers make the model-implied growth rate $\mu_U\eta_0^{-1} + 0.5\sigma_U^2\eta_0^{-1}\left(\eta_0^{-1}-1\right)$ and volatility $\sigma_U\eta_0^{-1}$ of operating income in the data-breach-free scenario match empirical counterparts calculated from TJX operating income data during 1960-2006 (the corresponding observed growth rate and volatility respectively equal 21.575% and 39.944%).[16]

We now move attention to the lower bounds of the product demand growth rate, product demand volatility, and the price elasticity of customers. These three parameters reflect the post-data-breach outlook for product demand. Similar to ε_U, we calibrate ε_L from the corresponding formula:

$$\xi_{all}(i) = \frac{1}{1-\gamma^{-1}+\frac{\gamma^{-1}}{1-\varepsilon_i}} + \frac{2}{1-\gamma^{-1}} = \frac{1}{1-\gamma^{-1}+\frac{\gamma^{-1}}{1-\varepsilon_L-(\varepsilon_U-\varepsilon_L)(1-\varpi)^i}} + \frac{2}{1-\gamma^{-1}} \tag{7}$$

[13] We additionally provide an example of performing our calibration strategies based on a broad firm sample. Related details are presented in Online Appendix. Using this alternative set of parameter values does not alter our main results on the comparative statics of cyber insurance premiums

[14] Details about the technical derivation for equations (5) and (7) are given in Appendix D.

[15] We formulate our regression specification (6) by following Doerrenberg et al. (2017) and Neisser (2021). For brevity, we do not consider control variables. Controlling for firm characteristics might alter the value of the estimated elasticity of sales revenue but does not alter our main results on the comparative statics of cyber insurance premiums.

[16] The model-implied operating income growth rate and volatility conditional on the data-breach-free scenario are derived using Ito's lemma and expression (3) (given $t < \overline{T}_1$).

where ξ_{all} is the unconditional elasticity of sales revenue to the markup pricing rate. This will be estimated from regression specification (6) (need to replace ξ_{pre} in (6) with ξ_{all}) for *full-period* data on TJX's corresponding accounting variables. We then choose ε_L at 1.01, which makes the expected unconditional elasticity of sales revenue $\mathbb{E}_0^{\mathbb{Q}} \xi_{all}(i)$ calculated from (7) match the afore -mentioned empirical counterpart estimated from (6); namely, $\xi_{all} = -1.410$.[17] Finally, we set the lower bounds of the product demand growth rate μ_L and of product demand volatility σ_L to be -6.1% and 21.25%, respectively. These align the first two simulated moments of operating income (equation (3)) generated by our model with empirical counterparts calculated from TJX's full-period operating income data (TJX's observed growth rate and volatility for operating income during 1960 -2019 are 18.976% and 35.752%, respectively).[18]

5.3. Insurance contract parameters

Consider now the rest of parameters. We choose the coverage rate ϕ at 50%, the expiration date T at 1 year, the knock-in barrier of the number of cyber event occurrences $(\overline{L}, \widetilde{L})$ at 1, the knock-out barrier of the number of cyber event occurrences $(\overline{U}, \widetilde{U})$ at ∞, the knock-in barrier of the virus-attack gravity x_L at 0%, and the knock-out barrier of the virus-attack gravity x_U at 100%. Our results only vary quantitatively (not qualitatively) with these contractual parameters. We will put a special focus on the influence of changes in the contract terms (e.g., deductibles, coverage limits, etc.) on cyber insurance premiums in a subsequent separate section. The subjective discount rate r is chosen at a relatively high level of 25%. This choice ensures compliance with the condition that the discount rate must exceed the expected growth rate of operating income, which aligns with the TJX's average operating income growth rate of approximately 20%. Under such a condition, the firm's expected value, as calculated from our formula, remains nonnegative.[19]

For convenience in inspecting our parameter calibration results, we compile them in Table 1.

Table 1
A Summary of Baseline Parameters.

Parameter Value	Parameter Definition	Type
Panel A: Cyber Events		
$\lambda_I = 20\,\%$	Intensity of type I cyber risk	Market-level
$\lambda_{II} = 11.008\,\%$	Intensity of type II cyber risk	Market-level
$\alpha = 58.004\,\%$	Probabilistic parameter of the virus-attack gravity	Country-level
$\beta = 9.99\,\%$	Probabilistic parameter of the virus-attack gravity	Country-level
$\boldsymbol{c} = \$2.837$	Recovery cost parameter	Firm-level
$\varpi = 20\,\%$	Premium customer loss rate	Market-level
Panel B: Firm Characteristics		
$\boldsymbol{Q} = 10$	Initial product demand	Normalized
$\boldsymbol{A} = 5$	Permanent production technology	Normalized
$\gamma = 40\,\%$	Return-to-scale parameter	Market-level
$\delta = 14.091\,\%$	Capital rental rate	Firm-level
$\varepsilon_U = 1.417$	Upper bound of the customer-to-price elasticity	Firm-level
$\varepsilon_L = 1.010$	Lower bound of the customer-to-price elasticity	Firm-level
$\mu_U = 29.473\,\%$	Upper bound of the product demand growth rate	Firm-level
$\mu_L = -6.1\%$	Lower bound of the product demand growth rate	Firm-level
$\sigma_U = 49.943\,\%$	Upper bound of product demand volatility	Firm-level
$\sigma_L = 21.25\,\%$	Lower bound of product demand volatility	Firm-level
Panel C: Insurance Contract Design		
$\phi = 50\%$	Coverage rate	Normalized
$T = 1$	Expiration date	Normalized
$\boldsymbol{r} = 25\%$	Subjective discount rate	Normalized
$x_U = 100\,\%$	Knock-out upper barrier of the virus-attack gravity	Normalized
$x_L = 0\,\%$	Knock-in lower barrier of the virus-attack gravity	Normalized
$\widetilde{U} = \infty$	Knock-out upper barrier of the number of type-I cyber event	Normalized
$\widetilde{L} = 1$	Knock-in lower barrier of the number of type-I cyber event	Normalized
$\overline{U} = \infty$	Knock-out upper barrier of the number of type-II cyber event	Normalized
$\overline{L} = 1$	Knock-in lower barrier of the number of type-II cyber event	Normalized

6. Quantitative results and empirical predictions

Section 6 discusses empirical predictions about cyber insurance valuation in three parts. The first part analyzes the influence of cyber risk changes on cyber insurance valuation. The second part will examine the implications of product market conditions for cyber insurance valuation. The third part focuses on the comparative statics of cyber insurance valuation regarding contractual parameters.

6.1. Cyber insurance premium and cyber risks

A consensus prediction underlying the insurance pricing literature is that the insured bearing a higher risk pays a higher premium for buying an insurance contract. Such a prediction is, however, only partially supported by our model. To examine the relation between cyber insurance premiums and cyber risks, we plot the total premium $I(0)$ against type-I cyber risk λ_I and type-II cyber risk λ_{II} in Fig. 3 and Fig. 4, respectively.

The two figures show that the influence of a rise in cyber risk intensity on the total premium is complex, and the direction of this influence is reversed by changes in the premium customer loss rate. When the premium customer loss rate is low (high), increasing the intensity of type-I and type-II cyber risk generates a positive (negative) and negative (positive) influence on the total premium, respectively. To further investigate, we plot the corresponding relative total premium against cyber risks in Panel B of Fig. 3 and Panels B and D of Fig. 4. We define the relative total premium as the total premium scaled by its corresponding baseline level (I at $\lambda_I = 20\%$ and $\lambda_{II} = 11.008\%$). As we observe in Panel B of Fig. 3, the slopes of the solid and dotted lines (with a higher premium customer loss rate) are negative, the dash-dotted line (a medium premium customer loss rate) has a U shape, and the slope of the dashed line (a low premium customer loss rate) is positive. Similar patterns appear in Panels B and D of Fig. 4. These results justify the relevance of the distinction between two cyber risk sources and of premium customers' aversion to data breaches in pricing cyber insurance. The complexity of the results above might arise from the fact that cyber insurance sub-premiums display asymmetric sensitivities to cyber risks. The magnitude of the influence of changes in the premium customer loss rate on these sensitivities is asymmetric as well.

To clarify how asymmetries in the sensitivities of sub-premiums shape the complexity of total premiums' sensitivity, we next move our attention to Figs. 5-7. These three figures plot cyber sub-premiums ($\widetilde{I}(0)$ and $\overline{I}(0)$) and their sensitivity to type-I and type-II cyber risk intensities.

[17] We calculate the expected unconditional elasticity of sales revenue by using the technique of simulation. Our simulation consists of 10,000 paths with a length of 60 years that matches the time span of TJX sample. On the basis of the weekly simulation frequency, each of path contains 3120 simulated-observation points.

[18] Our simulation presents that the annualized growth rate (volatility) of operating income is around 18.979% (35.7582%). The scheme of our simulation is identical to that described in footnote 17.

[19] Our formula is taken from Goldstein et al. (2001), which similarly impose the constraint that the discount rate exceeds the risk-adjusted EBIT growth rate on the calculations of firm value. The gap between these two rates implied by their parameter calibration equals 5.88%, close to our calibration results.

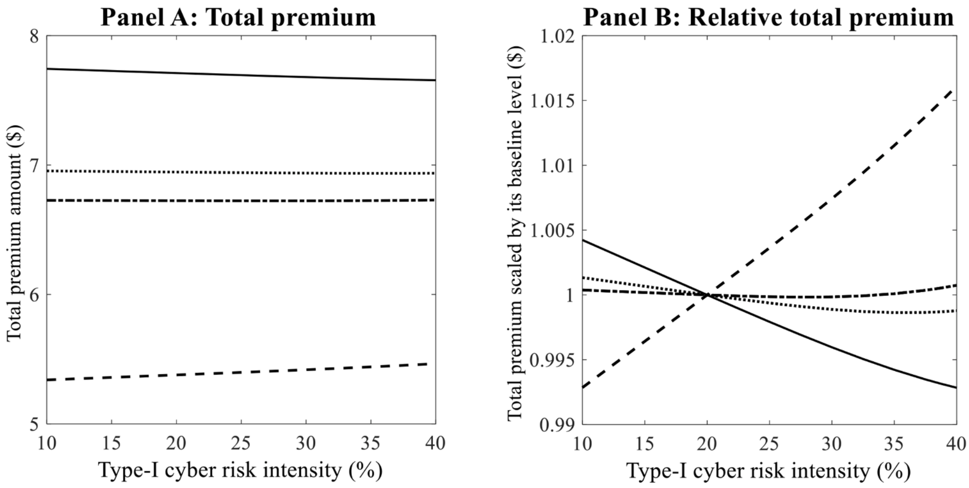

Fig. 3. Cyber insurance total premium against type-I cyber risk. The solid, dotted, dashed-dotted, and dashed lines are respectively plotted using the premium customer loss rate $\varpi = 20\%$, $\varpi = 16\%$, $\varpi = 15\%$, and $\varpi = 10\%$. The relative total premium equals the total premium scaled by its corresponding baseline level given $\lambda_I = 20\%$.

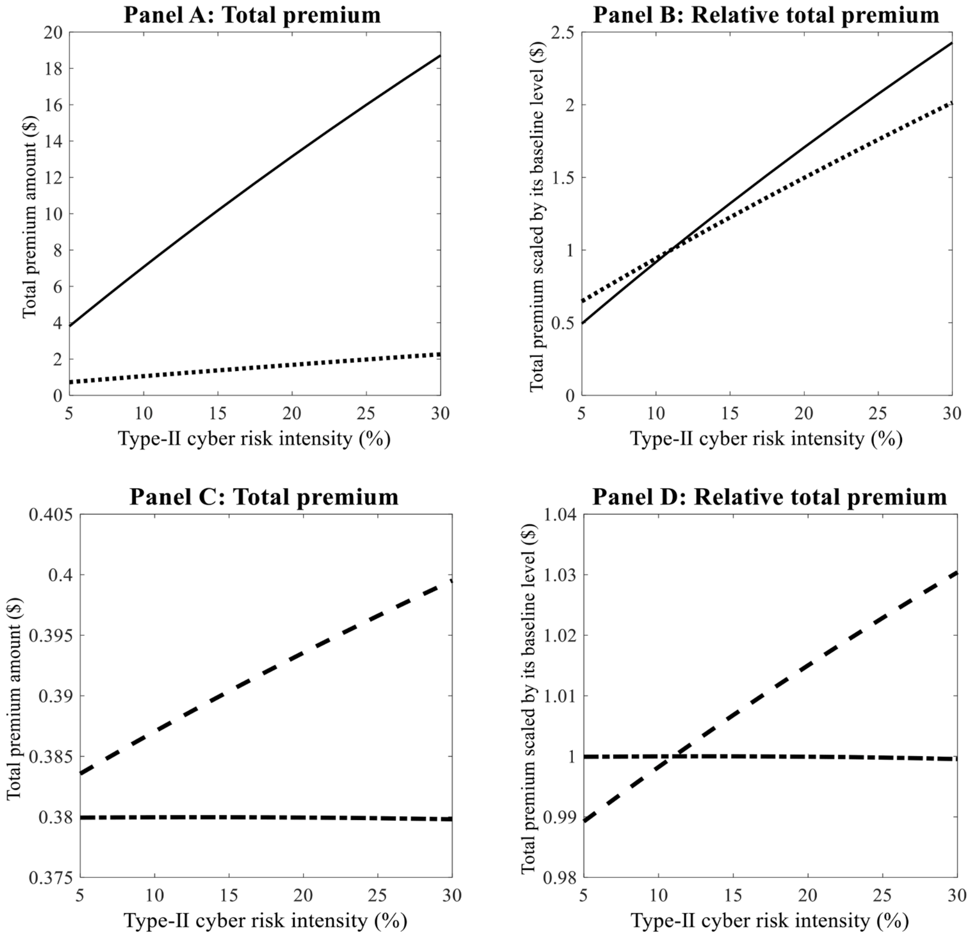

Fig. 4. Cyber insurance total premium against type-II cyber risk. The solid, dotted, dashed, and dash-dotted lines are plotted using the premium customer loss rate $\varpi = 20\%$, $\varpi = 1\%$, $\varpi = 10^{-4}$, and $\varpi = 10^{-6}$, respectively. The relative total premium is calculated as the total premium scaled by its corresponding baseline level given $\lambda_{II} = 11.008\%$.

The patterns present that the reactions of type-I sub-premium to changes in cyber risk intensity (see all lines in Panel A of Fig. 5 and Panels A, C, and E of Fig. 6) and those of type-II sub-premium to changes in cyber risk intensity (see all lines in Panel B of Fig. 5 and Panels B, D, and F of Fig. 6) do display asymmetric directions. The former reactions are weakly sensitive to changes in the premium customer loss rate, whereas the latter reactions are highly sensitive to such changes. For example, in Fig. 5, Panel A shows that the lines almost overlap given different levels of premium customer loss rates, while the slopes of the lines in Panel B increase as the premium customer loss rate decreases. In panel C the

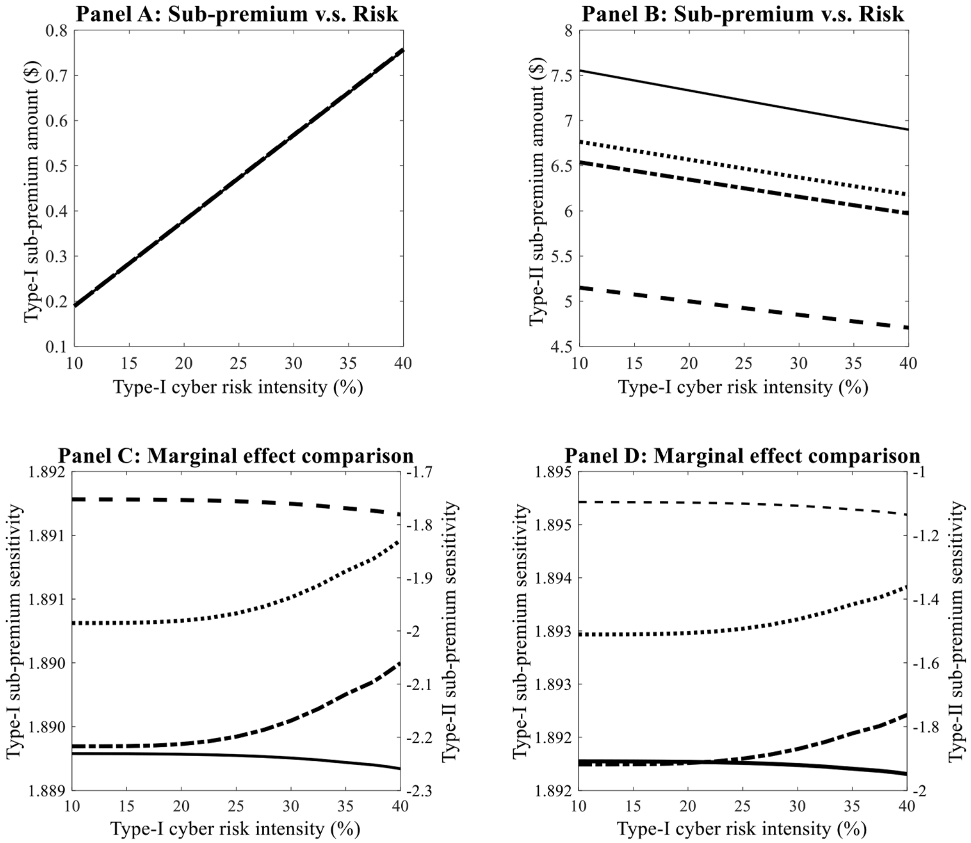

Fig. 5. Asymmetric sensitivities of cyber insurance sub-premiums to type-I cyber risk and the structure of related comparisons. In Panels A and B, the dashed, dash-dotted, dotted, and solid lines are respectively plotted setting $\varpi = 10\%$, $\varpi = 15\%$, $\varpi = 16\%$, and $\varpi = 20\%$. All lines in Panel A overlap. In Panel C, the solid and dashed (dash-dotted and dotted) lines plot the sensitivity of type-I (type-II) sub-premium to type-I cyber risk by using $\varpi = 20\%$ and $\varpi = 16\%$, respectively. In Panel D, the solid and dashed (dash-dotted and dotted) lines plot the sensitivity of type-I (type-II) sub-premium to type-I cyber risk intensity by using $\varpi = 15\%$ and $\varpi = 10\%$, respectively.

change in the sensitivity of type-I sub-premium to type-I cyber risk intensity seems limited as the premium customer loss rate falls from 20% (solid line) to 16% (dashed line), while the corresponding change in the sensitivity of type-II sub-premium is much greater (see the dashed-dotted and dotted lines). Similar patterns appear in Panel D and Fig. 7. It is notable that, while the arrivals of type-I events (virus attacks) and type-II events (data breaches) are mutually independent, both type-I and type-II sub-premiums are simultaneously influenced by changes in the cyber risk intensities of both types. A rise in the intensity of type-I cyber risk negatively affects the type-II sub-premium (see the negative slopes of the lines in Panel B of Fig. 5), because firms earn less profit from premium customers when suffering adverse shocks on productivity caused by virus attacks. The expected total compensation for operating income losses in the departures of premium customers due to data breaches falls as the frequency of virus attacks increases.

The influence of changes in type-II cyber risk intensity on type-I sub-premium is negative as well (see all lines in Panels A, C, and E of Fig. 6). The negative effect of a productivity shock due to virus attacks on a firm's operating income is in fact simultaneously affected by changes in product price competition and in the prospect of product demand. Premium customer departures make price competition weaker (means the price sensitivity of the customer base faced by firms lowers). Weak competition is favourable for firms suffering virus attacks, because adverse shocks on productivity cause firms to raise product prices. Decreases in price competition due to data breaches weaken the negative impact of virus attacks on firm operating income. Besides, the prospect of product demand worsens as premium customers leave. Expected operating income losses due to productivity shocks are less when the product demand growth rate is lower. An increase in the frequency of data breaches thus dilutes the expected negative influence of virus attacks on operating income. These two effects jointly shape an inverse association between type-II cyber risk and type-I sub-premium.

Asymmetries in the sensitivities of sub-premiums to cyber risks help clarify the complexity of the relation between total premium and cyber risks. Increasing type-I (type-II) cyber risk intensity delivers not only a usual positive effect on type-I (type-II) sub-premiums, but also a negative effect on type-II (type-I) sub-premiums. When the premium customer loss rate is high (low), the effect on type-II (type-I) sub-premiums dominates, and thus, the total premium positively correlates to type-II (type-I) cyber risk, but negatively to type-I (type-II) cyber risk.

6.2. *Cyber insurance premium and product markets*

We now examine the implications of product market conditions faced by the insured for cyber insurance valuation. We first focus on price competition (proxied by customers' price elasticity) and then on product demand characteristics; i.e., size, volatility, and the expected growth rate.

6.2.1. *Product price competition*

Fig. 8 plots the total premium against the upper bound of the price elasticity by holding fixed the effect of premium customers on price elasticity (the range of price elasticity $\varepsilon_U - \varepsilon_L$ is fixed). Similar to the cases of cyber risks, we find that the relation between price competition and the total premium is complex, and that the relation depends on the premium customer loss rate. This relation turns from U-shaped (the dotted line in Panel B of Fig. 8) to negative (the solid, dash-dotted, and

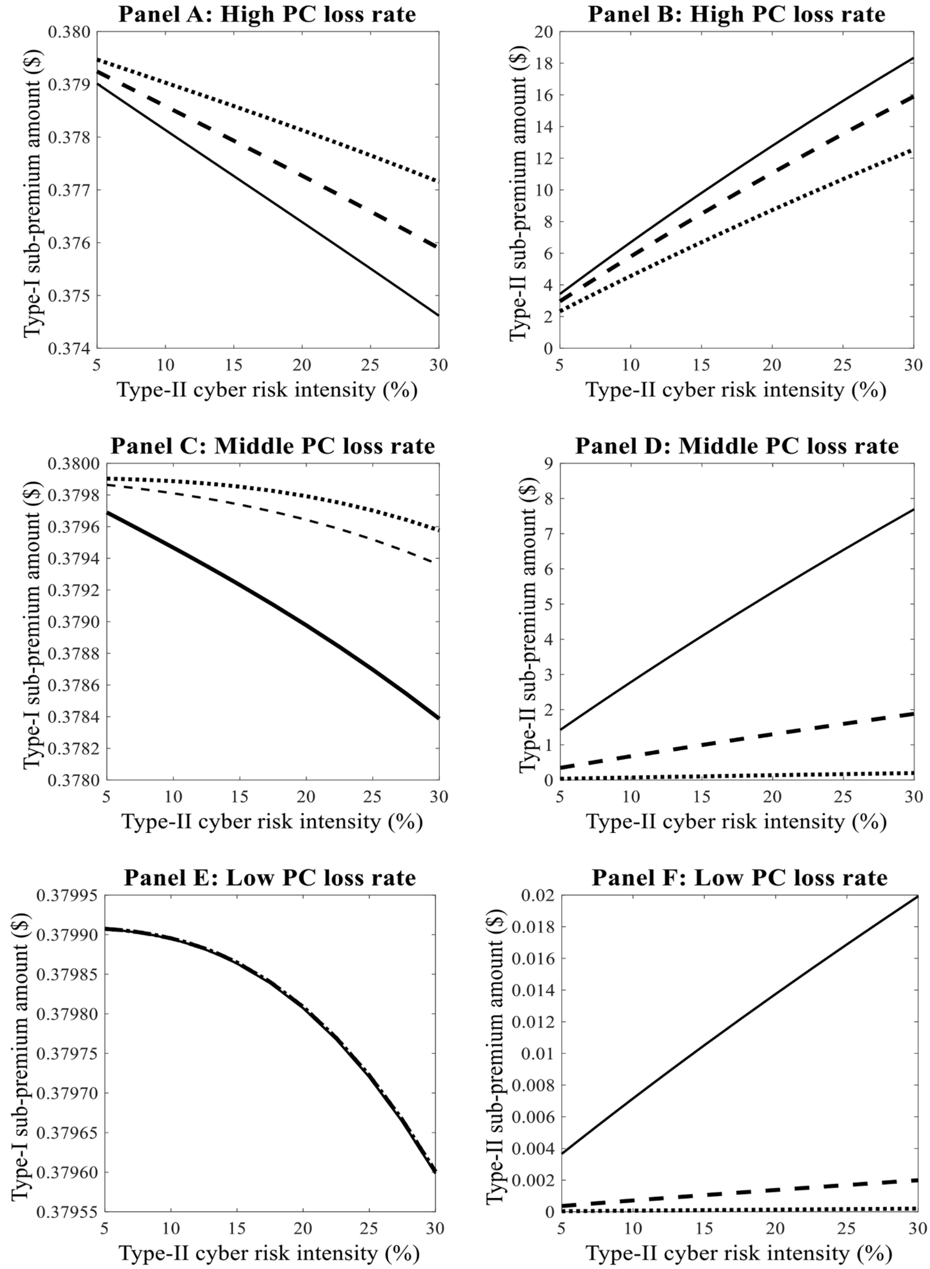

Fig. 6. Asymmetric sensitivities of cyber insurance sub-premiums to type-II cyber risk. In Panels A and B, the solid, dashed, and dotted lines are depicted using $\varpi = 20\%$, $\varpi = 15\%$, and $\varpi = 10\%$, respectively. In Panels C and D, the solid, dashed, and dotted lines are depicted using $\varpi = 5\%$, $\varpi = 1\%$, and $\varpi = 10^{-3}$, respectively. In Panels E and F, the solid, dashed, and dotted lines are plotted using $\varpi = 10^{-4}$, $\varpi = 10^{-5}$, and $\varpi = 10^{-6}$, respectively. All lines in Panel E overlap.

dashed lines in Panel B) when varying the premium customer loss rate from a low to high level.

Product price competition, in fact, affects the total premium in two ways. On the one hand, an increase in price competition enhances the negative effect of productivity shocks due to virus attacks on operating income. The reason is that firms suffering productivity shocks raise the product price temporarily (recall from Theorem 1 that the optimal price is decreasing in productivity technology), and that such a pricing strategy will discourage more customers if price competition is tougher. This enhancement effect generates a positive association between competition and type-I sub-premium (check all lines in Panel A of Fig. 9). On the other hand, because premium customers' patronage improves the prospect of product demand, firms absorb benefits delivered by premium customers through raising product prices (optimal product price increases with product demand). This suggests that as price competition rises, the available benefits from premium customers lower, and expected losses in operating income flows due to premium customer departures arising from data breaches decrease. Type-II sub-premium and price competition thus have an inverse relation (see all lines in Panel B of Fig. 9). Only if the premium customer loss rate is extremely low, the positive effect of competition on type-I sub-premium outweighs the negative effect on type-II sub-premium, causing a positive relationship between competition and total premium. In most of circumstances, the latter negative effect outweighs the former positive effect, and total premium decreases with competition.

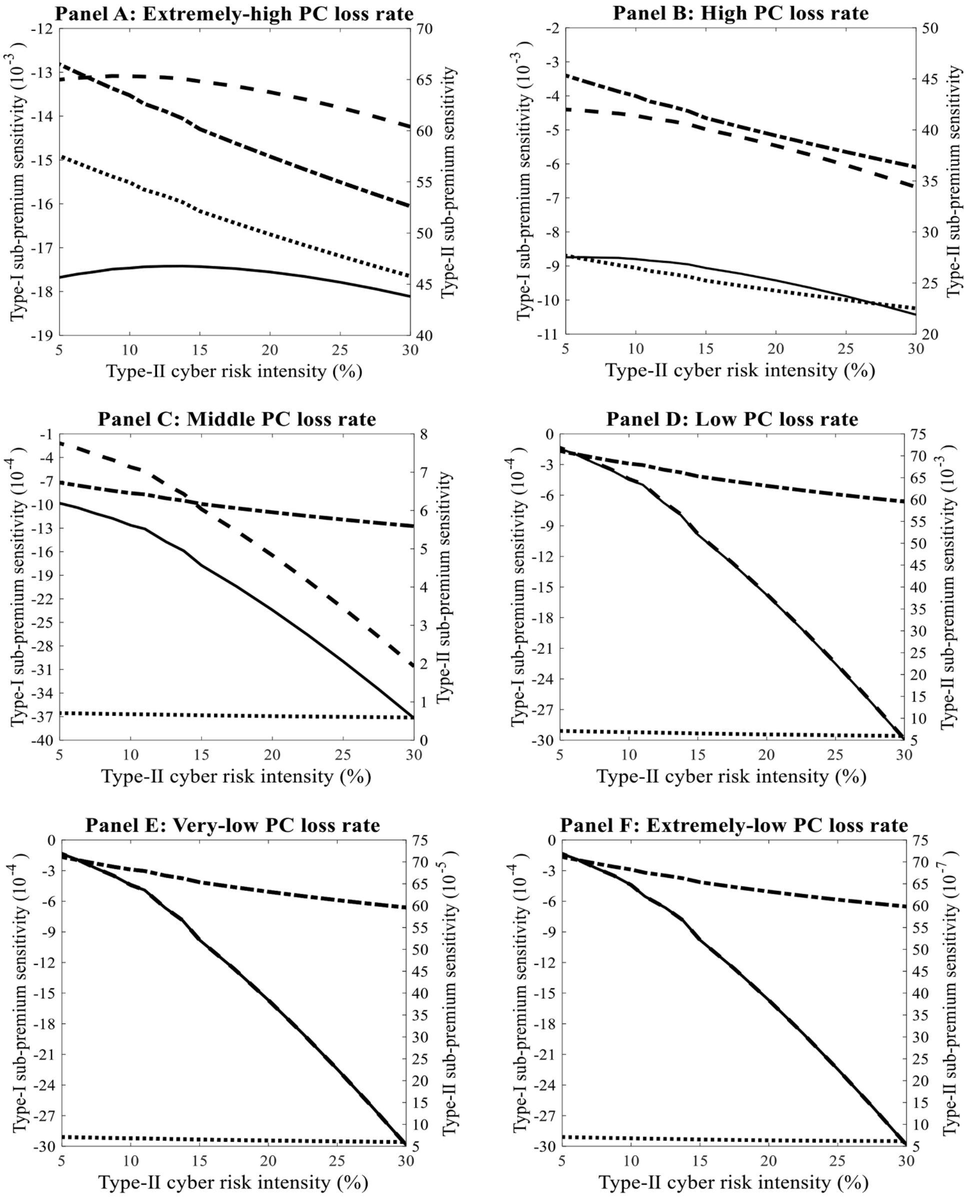

Fig. 7. Sensitivities of cyber insurance sub-premiums to type-II cyber risk under different levels of the premium customer loss rate. The solid and dashed (dash-dotted and dotted) lines plot the sensitivity of type-I (type-II) sub-premium to type-II cyber risk intensity. The solid and dash- dotted lines in Panels A, B, C, D, E, and F are respectively plotted choosing $\varpi = 20\%$, $\varpi = 10\%$, $\varpi = 1\%$, $\varpi = 10^{-4}$, $\varpi = 10^{-6}$, and $\varpi = 10^{-8}$; while the dashed and dotted lines are plotted choosing $\varpi = 15\%$, $\varpi = 5\%$, $\varpi = 10^{-3}$, $\varpi = 10^{-5}$, $\varpi = 10^{-7}$, and $\varpi = 10^{-9}$, respectively. In Panels D and F, the solid and dashed lines overlap.

6.2.2. *Product demand dynamics*

Consider next the influence of changes in product demand characteristics on cyber insurance valuation. We depict the total premium against the upper bound of the product demand growth rate and product demand volatility in Figs. 10 and 11, respectively, by holding the effects of premium customers on product demand dynamics fixed (the sizes of the dispersions $\mu_U - \mu_L$ and $\sigma_U - \sigma_L$ remain fixed). Fig. 12 plots the total premium against initial product demand.

As we can see, the slopes of all lines are consistently positive in Figs. 10 and 12 and negative in Fig. 11. These patterns suggest that insurance companies can charge a higher premium for cyber insurance when product demand faced by the insured firm is less volatile, grows faster, and has a larger size. Such results are consistent with our expectations. A decline in product demand volatility, a rise in the product demand growth rate, or an increase in the size of product demand gives rise to improvements in the conditions of product demand. Such improvements enable firms (insured firms) to earn more operating income. At the same time, marginal operating income loss in cyber events becomes larger. Firms facing better product demand conditions thus have stronger incentives to hedge cyber losses, and insurers under such circumstances tend to charge a higher premium.

6.3. *Cyber insurance premium and contract design*

We finally discuss the comparative statics of cyber insurance premium with respect to various contractual parameters. For convenience in subsequent discussions, we summarize the related results in Table 2. It is observable that insurance companies charge a higher premium for cyber insurance with a higher coverage rate or a longer expiration date. Such results are not beyond our expectations, because the expected value of coverage provided by a cyber insurance contract naturally increases with the coverage rate and contractual horizon. Also, we observe that the inclusions of deductibles and coverage upper limits both make cyber insurance cheaper. The effect of deductibles is proxied by the

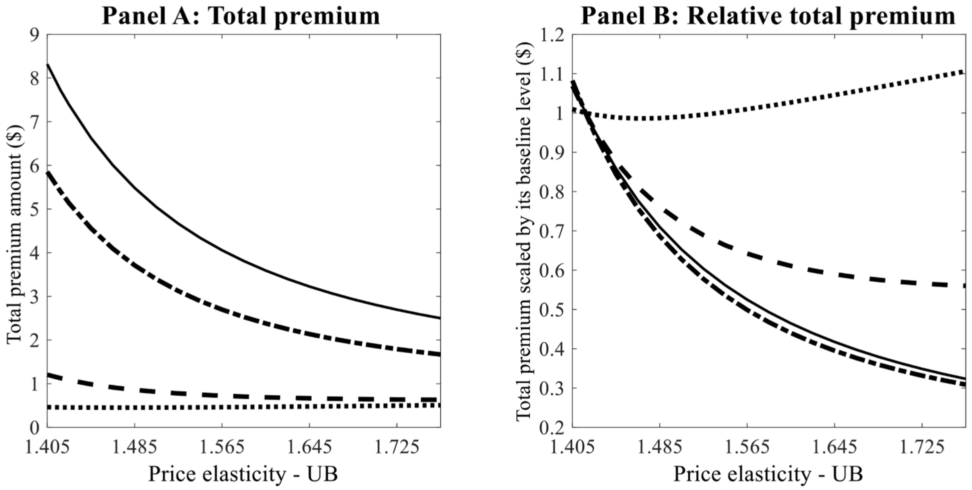

Fig. 8. Cyber insurance total premium and product price competition. The solid, dash-dotted, dashed, and dotted lines are respectively plotted using $\varpi = 20\%$, $\varpi = 10\%$, $\varpi = 1\%$, and $\varpi = 10^{-3}$. The relative total premium is computed as the total premium divided by its corresponding baseline level at $\varepsilon_U = 1.417$.

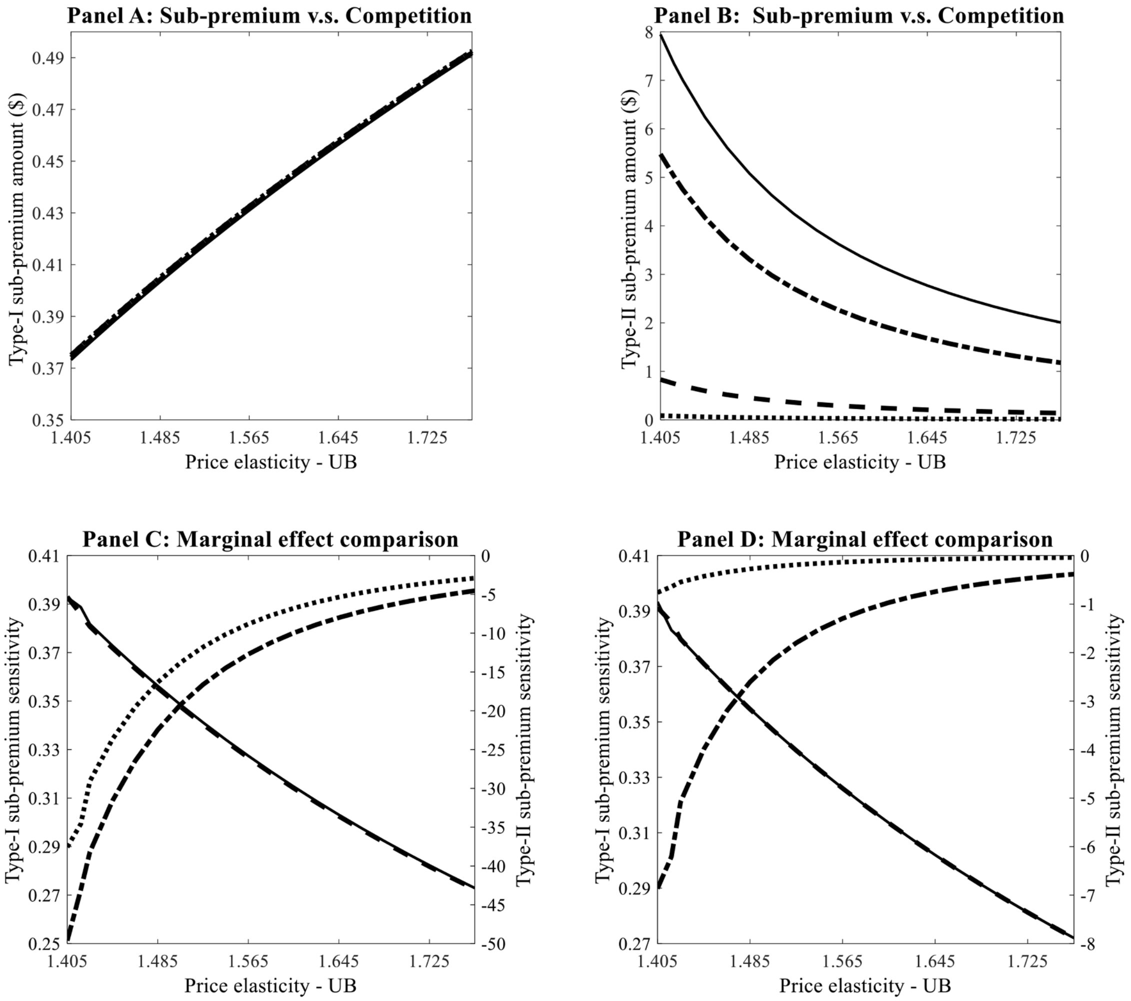

Fig. 9. Asymmetric sensitivities of cyber insurance sub-premiums to price competition. In Panels A and B, the dotted, dashed, dash-dotted, and solid lines are respectively plotted choosing $\varpi = 0.1\%$, $\varpi = 1\%$, $\varpi = 10\%$, and $\varpi = 20\%$ (all lines in Panel A overlap). In Panel C, the solid and dashed (dash-dotted and dotted) lines plot the sensitivity of type-I (type-II) sub-premium to the upper bound (UB) of price elasticity against the UB of price elasticity by choosing $\varpi = 20\%$ and $\varpi = 10\%$, respectively. In Panel D, the solid and dashed (dash-dotted and dotted) lines depict the sensitivity of type-I (type-II) sub-premium to the UB of price elasticity against the UB of price elas- ticity by choosing $\varpi = 1\%$ and $\varpi = 0.1\%$, respectively. In Panels C and D, the solid and dashed lines overlap. The dispersion of price elasticity (i.e., $\varepsilon_U - \varepsilon_L$) remains fixed when plotting the lines. Except for indicated parameters, all model parameters are chosen at their baseline levels.

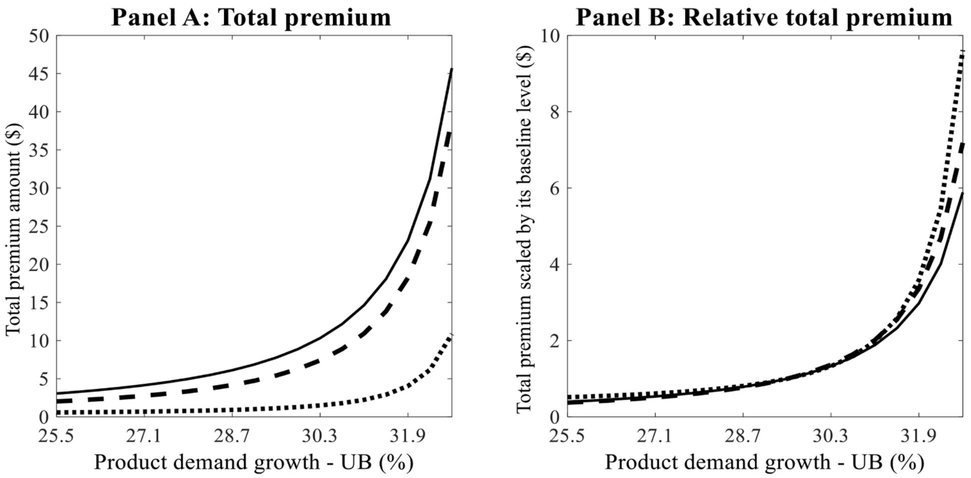

Fig. 10. Cyber insurance total premium and expected product demand growth. All lines plot the total premium or relative total premium against the upper bound of the product demand growth rate by holding the dispersion of the product demand growth rate $\mu_U - \mu_L$ fixed. The relative total premium equals the total premium scaled by its corresponding baseline level given $\mu_U = 29.473\%$. The solid, dashed, and dotted lines are plotted using $\varpi = 20\%$, $\varpi = 10\%$, and $\varpi = 1\%$, respectively.

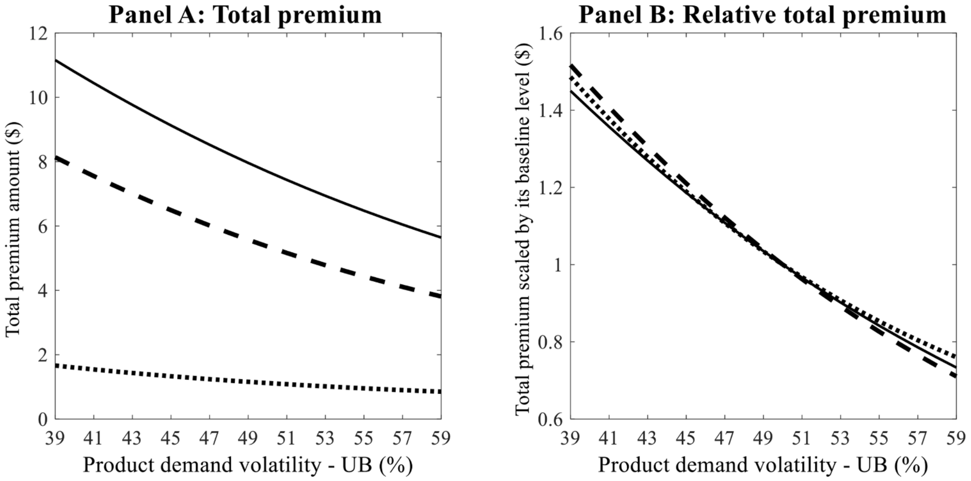

Fig. 11. Cyber insurance total premium and product demand volatility. The solid, dashed, and dotted lines are respectively plotted choosing $\varpi = 20\%$, $\varpi = 10\%$, and $\varpi = 1\%$. All lines plot the total premium or relative total premium against the upper bound of product demand volatility by holding the dispersion of product demand volatility $\sigma_U - \sigma_L$ fixed. The relative total premium is calculated as the total premium divided by its corresponding baseline level given $\sigma_U = 49.943\%$.

knock-in lower barriers of the number of cyber-event occurrences and of virus-attack gravity, while that of coverage limits is embodied by the corresponding knock-out upper barriers. Increasing (decreasing) these lower (upper) barriers causes a lower cyber insurance premium. Such results arise from the fact that both deductibles and coverage limits lower the amount of compensation for cyber losses promised by cyber insurance through narrowing the scope of insurance coverage.

6.3.1. *Conclusion*

This paper offers a novel model for quantifying firms' losses in cyber events and applies it to cyber insurance valuation. Our model implications deliver several new insights into cyber insurance valuation concerning cyber risk and product market conditions faced by firms. First, we find that the consensus prediction about the positive risk-premium relationship is no longer valid in our model. Premium customer loss due to data breaches and asymmetries in the sensitivities of cyber insurance sub-premiums to cyber risks from different sources jointly shape the complexity of the relationship between cyber insurance total premium and cyber risks. Second, in response to an increase in product price competition, cyber insurance premium varies, depending on the degree of premium customers' aversion to data breaches. Increasing price competition leads to a negative (positive) effect on sub-premiums involving losses due to data breaches (virus attacks). When the degree of aversion to data breaches is high (low), the negative (positive) effect dominates, and therefore, the total premium decreases (increases) with price competition. Third, firms facing a better prospect of their product demand have a stronger incentive to hedge losses in cyber events, meaning that insurance companies under such circumstances can charge

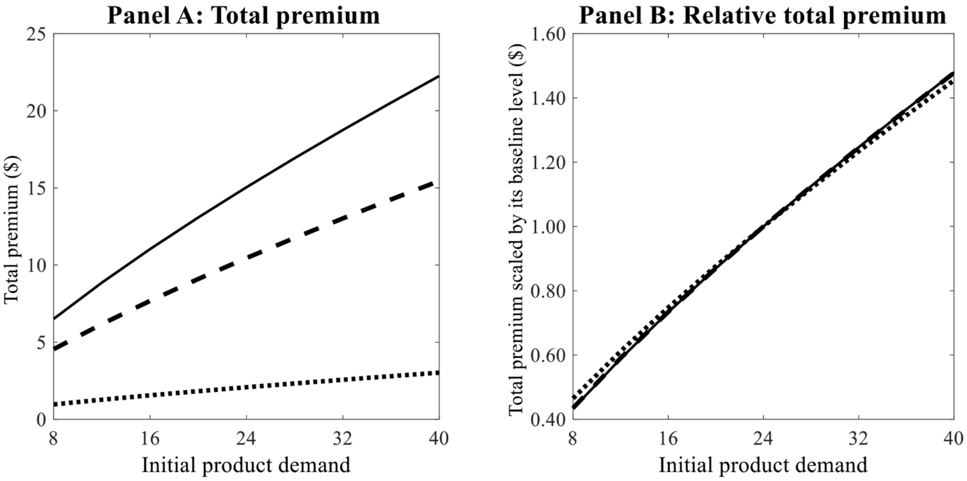

Fig. 12. Cyber insurance total premium against product demand size. The solid, dashed, and dotted lines are respectively plotted using $\varpi = 20\%$, $\varpi = 10\%$, and $\varpi = 1\%$. The relative total premium equals the total premium divided by its median level given $Q_d(0) = 24$.

Table 2
Premium Comparative Statics with Respect to Contractual Parameters.

Parameter Choices	Total Premium ($)	Change rate (%)	Type I Sub-premium ($)	Change rate (%)	Type II Sub-Premium ($)	Change rate (%)
Baseline	7.711	—	0.378	—	7.333	—
x_L=30%	7.710	-0.005	0.378	-0.107	7.333	0.000
x_L=40%	7.703	-0.101	0.370	-2.055	7.333	0.000
x_U=70%	7.650	-0.783	0.318	-15.980	7.333	0.000
x_U=80%	7.702	-0.112	0.369	-2.286	7.333	0.000
$\widetilde{L}$=1	7.350	-4.675	0.017	-95.380	7.333	0.000
$\widetilde{L}$=2	7.333	-4.901	0.000	-99.992	7.333	0.000
$\widetilde{U}$=2	7.351	-4.671	0.018	-95.283	7.333	0.000
$\widetilde{U}$=3	7.351	-4.671	0.018	-95.283	7.333	0.000
$\overline{L}$=1	7.711	0.000	0.378	0.000	7.333	0.000
$\overline{L}$=2	0.385	-95.008	0.378	0.000	0.007	-99.905
$\overline{U}$=2	7.711	0.000	0.378	0.000	7.333	0.000
$\overline{U}$=3	7.711	0.000	0.378	0.000	7.333	0.000
ϕ=40%	6.169	-20.000	0.302	-20.000	5.866	-20.000
ϕ=60%	9.253	20.000	0.454	20.000	8.799	20.000
T=3	20.128	161.040	1.008	166.798	19.119	160.743
T=5	29.500	282.584	1.511	299.669	27.989	281.704

Table 2 shows the comparative statics of cyber insurance premiums across various combinations of contractual parameters, including the coverage rate, expiration date, knock-out and knock-in barriers for virus-attack gravity, and knock-out and knock-in barriers for the number of occurrences of cyber events. The first, third, and fifth columns (from left to right) respectively report the cyber insurance total premiums, type-I sub-premiums, and type-II sub-premiums; while the second, fourth, and sixth columns (from left to right) present corresponding percentage changes in these premiums relative to the baseline case.

a higher premium for cyber insurance.

CRediT authorship contribution statement

Chang-Chih Chen: Formal analysis, Data curation, Conceptualization. **Chia-Chien Chang:** Resources, Project administration, Methodology. **Ying Rui:** Validation. **Min-Teh Yu:** Writing – review & editing, Validation, Supervision, Investigation.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.jbankfin.2025.107564.

Appendix A. Comparison among Various Cyber Insurance Pricing Models

The comparison contains MSCMP (Mukhopadhyay et al., 2005), BK (Böhme and Kataria, 2006), MCSMS (Mukhopadhyay et al., 2013), HH (Herath and Herath, 2007, 2011), SLLLC (Su et al., 2021), FWW (Fahrenwaldt et al., 2018), XH (Xu and Hua, 2019), and our model.

Model feature	Cyber Risk Source		Cyber Event Frequency			Cyber Loss Measurement/Quantification			Parameterization			Numerical Implementation		
Model type	Virus or hacking	Data breach	Poisson	Beta-binomial	Unspecified	Artificially designed form	Exogenous SPs/RVs	Endogenous structural form	Calib.	Estima.	Arbi. choice	Analytical formulae	Simulations	N. A.
MSCMP	•				•	•					•			•
BK	•			•		•					•			•
MCSMS	•				•	•			•					•
HH	•		•				•			•			•	
SLLLC	•		•				•			•			•	
FWW	•		•				•				•		•	
XH		•	•				•				•		•	
Ours	•	•	•					•	•	•		•		

Note: “Exogenous SPs/RVs” refers to the case where cyber losses are specified as exogenous stochastic processes/random variables. “Calib”, “Estima”, and “Arbi choice” refer to the case where the baseline parameters are calibrated from the literature or empirical data, estimated using goodness-of-fit tests, and based on arbitrary choices, respectively.

Appendix B. Proof of Theorem 2

For notational convenience, we first define:

$$\varepsilon_i \equiv \varepsilon_L + (\varepsilon_U - \varepsilon_L)(1-\varpi)^i, \text{if } i = 0,1,2\cdots\infty; \mu_i \equiv \mu_L + (\mu_U - \mu_L)(1-\varpi)^i, \text{if } i = 0,1,2\cdots\infty;$$

$$\sigma_i \equiv \sigma_L + (\sigma_U - \sigma_L)(1-\varpi)^i, \text{if } i = 0,1,2\cdots\infty; \eta_i \equiv \varepsilon_i + \gamma - \gamma\varepsilon_i, \text{ifi} = 0,1,2\cdots\infty;$$

$$\Xi(a,b) \equiv A^{(a-1)/b}\left(\frac{\delta a}{a-b}\right)^{1-a/b}\frac{b}{a};$$

$$\xi(l,m,n,u,v) \equiv \left(m + 0.5n^2\left(l^{-1}-1\right)\right)l^{-1}(v-u);$$

$$\mathscr{F}^d_t = \sigma(Q_d(s), 0 \le s \le t);$$

$$\widetilde{\mathscr{H}}^i_t = \sigma\left(1_{(\tilde{I}_i>s)}, 0 \le s \le t\right);\ \overline{\mathscr{H}}^i_t = \sigma\left(1_{(\bar{I}_i>s)}, 0 \le s \le t\right).$$

Taking the expectation of compensation for i^{th} type-I cyber loss as an example, we have:

$$\mathbb{E}^Q_0\ \phi\ \widetilde{L}(\widetilde{T}_i)e^{-r\tilde{T}_i}\ 1_{(\tilde{T}_i\le T)}1_{(x_L\le x_i\le x_U)} = \mathbb{E}^Q_0\ \phi\ \widetilde{L}(\widetilde{T}_i)e^{-r\tilde{T}_i}\ 1_{(\tilde{T}_i\le T)}1_{(x_L\le x_i\le x_U)}\sum_{j=0}^{\infty} 1_{\left(T_j\le\tilde{T}_i<T_{j+1}\right)}.$$

Consider the intermediate term $\mathbb{E}^Q_0\ \phi\ \widetilde{L}(\widetilde{T}_i)e^{-r\tilde{T}_i}\ 1_{(\tilde{T}_i\le T)}1_{(x_L\le x_i\le x_U)}1_{\left(\overline{T}_j\le\tilde{T}_i<\overline{T}_{j+1}\right)} \equiv \widetilde{V}(i,j)$, and plugging

$$\widetilde{L}(\widetilde{T}_i) = Q_d(\widetilde{T}_i)^{1/\eta(\tilde{T}_i)}\ \boldsymbol{A}^{(\varepsilon(\tilde{T}_i)-1/\eta(\tilde{T}_i))}\left(\frac{\delta\varepsilon(\widetilde{T}_i)}{\varepsilon(\widetilde{T}_i)-\eta(\widetilde{T}_i)}\right)^{1-\varepsilon(\tilde{T}_i)/\eta(\tilde{T}_i)}\frac{\eta(\widetilde{T}_i)}{\varepsilon(\widetilde{T}_i)}(1-(1-x_i))^{(\varepsilon(\tilde{T}_i)-1)/\eta(\tilde{T}_i)} + x_i\ \boldsymbol{c}$$

into this intermediate term yields:

$$\widetilde{V}(i,j) = \mathbb{E}^Q_0\left[\phi\left(Q_d(\widetilde{T}_i)^{1/\eta_j}\ \Xi\left(\varepsilon_j,\eta_j\right)\left(1-(1-x_i)^{\left(\varepsilon_j-1\right)/\eta_j}\right)+x_i\boldsymbol{c}\right)\ e^{-r\tilde{T}_i}\ 1_{(\tilde{T}_i\le T)}1_{(x_L\le x_i\le x_U)}1_{\left(\overline{T}_j\le\overline{T}_i<\overline{T}_{j+1}\right)}\right].$$

Since $\widetilde{T}_i < \overline{T}_{j+1}$ and $Q_d(\widetilde{T}_i) = Q_d(\overline{T}_j)\,e^{\left(\mu_j-\ 0.5\ \sigma_j^2\right)\left(\tilde{T}_i-\overline{T}_j\right)+\sigma_j\left(B(\tilde{T}_i)-B\left(\overline{T}_j\right)\right)}$, we use Tower law and have

$$\begin{aligned}
\widetilde{V}(i,j) &= \mathbb{E}^Q_0\ \left[\mathbb{E}^Q\left[\phi\left(Q_d(\widetilde{T}_i)^{1/\eta_j}\ \Xi\left(\varepsilon_j,\eta_j\right)\left(1-(1-x_i)^{\left(\varepsilon_j-1\right)/\eta_j}\right)+x_i\ \boldsymbol{c}\right)\ e^{-r\ \tilde{T}_i}\right.\right.\\
&\times 1_{(\tilde{T}_i\le T)}\ 1_{(x_L\le x_i\le x_U)}\ 1_{\left(\overline{T}_j\le\tilde{T}_i\le\overline{T}_{j+1}\right)}\left|\mathscr{F}^x_i\vee\mathscr{F}^d_{\overline{T}_j}\vee\widetilde{\mathscr{H}}^i_T\vee\overline{\mathscr{H}}^1_T\vee\overline{\mathscr{H}}^2_T\vee\cdots\vee\overline{\mathscr{H}}^{j+1}_T\right]\right]\\
&= \mathbb{E}^Q_0\left[\left[\mathbb{E}^Q\left[Q_d(\widetilde{T}_i)^{1/\eta_j}\middle|\mathscr{F}^x_i\vee\mathscr{F}^d_{\overline{T}_j}\vee\widetilde{\mathscr{H}}^i_T\vee\overline{\mathscr{H}}^1_T\vee\overline{\mathscr{H}}^2_T\vee\cdots\vee\overline{\mathscr{H}}^{j+1}_T\right]\ \Xi\left(\varepsilon_j,\eta_j\right)\right.\right.\\
&\quad\times\left(1-(1-x_i)^{\left(\varepsilon_j-1\right)/\eta_j}\right)+x_i\ \boldsymbol{c}\Big]\ \phi\ e^{-r\tilde{T}_i}\ 1_{(\tilde{T}_i\le T)}1_{(x_L\le x_i\le x_U)}1_{\left(\overline{T}_j\le\tilde{T}_i<\overline{T}_{j+1}\right)}\Big]\\
&= \mathbb{E}^Q_0\Big[\ \phi\ \left(Q_d\left(\overline{T}_j\right)^{1/\eta_j}\ e^{\xi\left(\eta_j,\mu_j,\sigma_j,\overline{T}_j,\tilde{T}_i\right)}\ \Xi\left(\varepsilon_j,\eta_j\right)\left(1-(1-x_i)^{\left(\varepsilon_j-1\right)/\eta_j}\right)+x_i\ \boldsymbol{c}\right)\\
&\qquad\times e^{-r\tilde{T}_i}\ 1_{(\tilde{T}_i\le T)}1_{(x_L\le x_i\le x_U)}1_{\left(\overline{T}_j\le\tilde{T}_i<\overline{T}_{j+1}\right)}\Big].
\end{aligned}$$

We continue by repeatedly applying the law of iterated expectation, which leads to

$$\begin{aligned}
\widetilde{V}(i,j) &= \mathbb{E}^Q_0\ \Big[\phi\ \left(Q_d\left(\overline{T}_{j-1}\right)^{1/\eta_j}\ e^{\xi\left(\eta_j,\mu_j,\sigma_j,\overline{T}_j,\tilde{T}_i\right)+\xi\left(\eta_j,\mu_{j-1},\sigma_{j-1},\overline{T}_{j-1},\overline{T}_j\right)}\ \Xi\left(\varepsilon_j,\eta_j\right)\left(1-(1-x_i)^{\left(\varepsilon_j-1\right)/\eta_j}\right)+x_i\ \boldsymbol{c}\right)\\
&\qquad\times e^{-r\tilde{T}_i}\ 1_{(\tilde{T}_i\le T)}1_{(x_L\le x_i\le x_U)}1_{\left(\overline{T}_j\le\tilde{T}_i<\overline{T}_{j+1}\right)}\Big]
\end{aligned}$$

We then have:

$$\widetilde{V}(i,j) = \mathbb{E}_0^Q\left[\phi\left(Q^{1/\eta_j}\ \mathrm{e}^{\xi\left(\eta_j,\mu_j,\sigma_j,\overline{T}_j,\tilde{T}_i\right)+\sum_{k=1}^{j}\xi\left(\eta_j,\mu_{k-1},\sigma_{k-1},\overline{T}_{k-1},\overline{T}_k\right)}\ \Xi\left(\varepsilon_j,\eta_j\right)\left(1-(1-x_i)^{\left(\varepsilon_j-1\right)/\eta_j}\right)+x_i\ \boldsymbol{c}\right)\right.$$

$$\times e^{-r\tilde{T}_i}\ 1_{(\tilde{T}_i\le T)}1_{(x_L\le x_i\le x_U)}1_{\left(\overline{T}_j\le\tilde{T}_i\le\overline{T}_{j+1}\right)}$$

$$= \int_0^T\int_{t_1}^T\int_{t_2}^T\cdots\int_{t_j}^T\int_t^\infty\int_{x_L}^{x_U}\left(Q^{1/\eta_j}\ \mathrm{e}^{\xi\left(\eta_j,\mu_j,\sigma_j,t_j,t_i\right)+\sum_{k=1}^{j}\xi\left(\eta_j,\mu_{k-1},\sigma_{k-1},t_{k-1},t_k\right)}\ \left(1-(1-z)^{\left(\varepsilon_j-1\right)/\eta_j}\right)\right.$$

$$\times\ \Xi\left(\varepsilon_j,\eta_j\right)+z\ \boldsymbol{c}\Big)e^{-rt}\,f_x(z)\,\widetilde{f}_i(t)\ \prod_{k=1}^{j+1}\overline{f}_k(t_k)\ dz\ dt_{j+1}dt\ dt_j\cdots dt_3\ dt_2\ dt_1$$

The generalized formula can therefore be summarized as:

$$\widetilde{V}(i,0) = \int_0^T\int_t^\infty\int_{x_L}^{x_U}\left(\boldsymbol{Q}^{1/\eta_0}\ \mathrm{e}^{\xi(\eta_0,\mu_0,\sigma_0,0,t_0)}\ \left(1-(1-z)^{(\varepsilon_0-1)/\eta_0}\right)\ \Xi(\varepsilon_0,\eta_0)+z\ \mathbf{c}\right)$$
$$\times\ \mathrm{e}^{-rt}\ \phi\ f_x(z)\ \widetilde{f}_i(t)\ \overline{f}_1(t_1)\ dz\ dt_1 dt;$$

$$\widetilde{V}(i,1) = \int_0^T\int_{t_1}^T\int_t^\infty\int_{x_L}^{x_U}\left(\boldsymbol{Q}^{1/\eta_1}\ \mathrm{e}^{\xi(\eta_1,\mu_1,\sigma_1,t_1,t)+\xi(\eta_1,\mu_0,\sigma_0,0,t_1)}\ \left(1-(1-z)^{(\varepsilon_1-1)/\eta_1}\right)\right.$$
$$\times\ \Xi(\varepsilon_1,\eta_1)+z\boldsymbol{c}\Big)\ \mathrm{e}^{-rt}\ \phi\ f_x(z)\,\widetilde{f}_i(t)\,\overline{f}_1(t_1)\ dz\ dt_2\ dt\ dt_1;$$

$$\widetilde{V}(i,2) = \int_0^T\int_{t_1}^T\int_{t_2}^T\int_t^\infty\int_{x_L}^{x_U}\left(\boldsymbol{Q}^{1/\eta_2}\ \mathrm{e}^{\xi(\eta_2,\mu_2,\sigma_2,t_2,t)+\xi(\eta_2,\mu_0,\sigma_0,0,t_1)+\xi(\eta_2,\mu_1,\sigma_1,t_1,t_2)}\ \Xi(\varepsilon_2,\eta_2)\right.$$
$$\times\left(1-(1-z)^{(\varepsilon_2-1/\eta_2)}\right)+z\ \boldsymbol{c}\Big)\ \mathrm{e}^{-rt}\ \phi\ f_x(z)\ \widetilde{f}_i(t)\ \prod_{k=1}^{3}\overline{f}_k(t_k)\ dz\ dt_3\ dt\ dt_2\ dt_1;$$

$$\widetilde{V}(i,j) = \int_0^T\int_{t_1}^T\int_{t_2}^T\cdots\int_{t_j}^T\int_t^\infty\int_{x_L}^{x_U}\ \phi\ \left(z\ \boldsymbol{c}+\boldsymbol{Q}^{1/\eta_j}\ \mathrm{e}^{\xi\left(\eta_j,\mu_j,\sigma_j,t_j,t\right)+\sum_{k=1}^{j}\xi\left(\eta_j,\mu_{k-1},\sigma_{k-1},t_{k-1},t_k\right)}\ \Xi\left(\varepsilon_j,\eta_j\right)\right.$$
$$\times\left(1-(1-z)^{\left(\varepsilon_j-1\right)/\eta_j}\right)\Big)\ e^{-rt}\ f_x(z)\,\widetilde{f}_i(t)\ \prod_{k=1}^{j+1}\overline{f}_k(t_k)\ dz\ dt_{j+1}\ dt\ dt_j\cdots dt_3\ dt_2\ dt_1;$$

which provide the formula for $\widetilde{I}(0)\ =\sum_{i=\tilde{L}}^{\tilde{U}-1}\sum_{j=0}^{\infty}\widetilde{V}(i,j)$.

Appendix C. Proof of Theorem 3

We similarly take the case of i^{th} type-II cyber loss as an example for illustration. For notational convenience, we define $\widetilde{f}_i(t,\ s)\ =\ \lambda_I\ \mathrm{e}^{-\lambda_I(t-s)}(\lambda_I(t-s))^{i-1}[(i-1)!]^{-1}$. It is known from equations (1)-(2) in Goldstein et al. (2001) that:

$$\mathbb{E}_{\overline{T}_{i-}}^{Q}\int_{\overline{T}_{i-}}^{\infty}\widehat{\pi}^*(Q_d(s),\ \boldsymbol{A})\ e^{-r(s-\overline{T}_{i-})}\ ds = Q_d(\overline{T}_{i-})^{1/\eta_{i-1}}\ \Xi(\varepsilon_{i-1},\eta_{i-1})(\boldsymbol{r}-\xi(\eta_{i-1},\mu_{i-1},\sigma_{i-1},0,1))^{-1};$$
$$\mathbb{E}_{\overline{T}_{i-}}^{Q}\int_{\overline{T}_{i-}}^{\infty}\widehat{\pi}^*(Q_d(s),\ \boldsymbol{A})\ e^{-r(s-\overline{T}_{i})}\ ds = Q_d(\overline{T}_{i})^{1/\eta_{i}}\ \Xi(\varepsilon_{i},\eta_{i})(\boldsymbol{r}-\xi(\eta_{i},\mu_{i},\sigma_{i},0,1))^{-1}.$$

Moreover, since $Q_d\left(\widetilde{T}_j\right)=Q_d\left(\overline{T}_{i-}\right)\mathrm{e}^{\left(\mu_{i-1}-0.5\,\sigma_{i-1}^2\right)\left(\tilde{T}_j-\overline{T}_{i-}\right)+\sigma_{i-1}\left(B\left(\tilde{T}_j\right)-B\left(\overline{T}_{i-}\right)\right)}$ (from Ito’s lemma) and $\widehat{\pi}^*\left(Q_d\left(\widetilde{T}_{j-}\right),\ A\left(\widetilde{T}_{j-}\right)\right)-\widehat{\pi}^*\left(Q_d\left(\widetilde{T}_j\right),\ A\left(\widetilde{T}_j\right)\right)\ =\ Q_d\left(\widetilde{T}_j\right)^{1/\eta_{i-1}}\ \Xi(\varepsilon_{i-1},\eta_{i-1})\left(1-\ (1-x_j)^{(\varepsilon_{i-1}-1)/\eta_{i-1}}\right)$, using the law of iterated expectation yields:

$$\mathbb{E}_{\overline{T}_{i-}}^{Q}\left(\widehat{\pi}*\left(Q_d\left(\widetilde{T}_{j-}\right),\ A\left(\widetilde{T}_{j-}\right)\right)-\widehat{\pi}*\left(Q_d\left(\widetilde{T}_j\right),\ A\left(\widetilde{T}_j\right)\right)\right)\ \mathrm{e}^{-r\left(\tilde{T}_j-\overline{T}_{i-}\right)}\ 1_{\left(\overline{T}_i<\tilde{T}_j\right)}$$
$$=\mathbb{E}_{\overline{T}_{i-}}^{Q}\ Q_d\left(\widetilde{T}_j\right)^{1/\eta_{i-1}}\ \boldsymbol{\Xi}(\varepsilon_{i-1},\eta_{i-1})\left(1-\left(1-x_j\right)^{(\varepsilon_{i-1}-1)/\eta_{i-1}}\right)\ \mathrm{e}^{-r\left(\tilde{T}_j-\overline{T}_{i-}\right)}\ 1_{\left(\overline{T}_i<\tilde{T}_j\right)}$$
$$=\mathbb{E}_{\overline{T}_{i-}}^{Q}\left[Q_d(\overline{T}_{i-})^{1/\eta_{i-1}}\ \mathrm{e}^{\xi\left(\eta_{i-1},\mu_{i-1},\sigma_{i-1},\overline{T}_{i-},\overline{T}_j\right)}\ \Xi(\varepsilon_{i-1},\eta_{i-1})\left(1-\left(1-x_j\right)^{(\varepsilon_{i-1}-1)/\eta_{i-1}}\right)\right.$$
$$\left.\times e^{-r\left(\overline{T}_j-\overline{T}_{i-}\right)}\ 1_{\left(\overline{T}_i<\tilde{T}_j\right)}\right]$$
$$=\int_{\overline{T}_i}^{\infty}\int_0^1\left(1-(1-z)^{(\varepsilon_{i-1}-1)/\eta_{i-1}}\right)\ \mathrm{e}^{\xi(\eta_{i-1},\mu_{i-1},\sigma_{i-1},\overline{T}_{i-},t)-r(t-\overline{T}_{i-})}\ f_x(z)\ \widetilde{f}_j(t,\overline{T}_{i-})\ dz\ dt$$
$$\times Q_d(\overline{T}_{i-})^{1/\eta_{i-1}}\ \Xi(\varepsilon_{i-1},\eta_{i-1})\equiv Q_d(\overline{T}_{i-})^{1/\eta_{i-1}}\ \Delta(\varepsilon_{i-1},\eta_{i-1},\mu_{i-1},\sigma_{i-1},\overline{T}_{i-},j)$$

The derivation above implies:

$$\mathbb{E}_{\overline{T}_{i-}}^{Q}\left(\widehat{\pi}^*\left(\widetilde{T}_{j-}\right)-\widehat{\pi}^*\left(\widetilde{T}_j\right)\right)\ \mathrm{e}^{-r\left(\overline{T}_j-\overline{T}_{i-}\right)}\ 1_{\left(\overline{T}_i<\tilde{T}_j\right)}\equiv Q_d(\overline{T}_{i-})^{1/\eta_{i-1}}\ \Delta(\varepsilon_{i-1},\eta_{i-1},\mu_{i-1},\sigma_{i-1},\overline{T}_{i-},j);$$

which further delivers:

$$\mathbb{E}_{\overline{T}_{i}}^{Q}\left(\widehat{\pi}^*\left(\widetilde{T}_{j-}\right)-\widehat{\pi}^*\left(\widetilde{T}_j\right)\right)\ \mathrm{e}^{-r\left(\overline{T}_j-\overline{T}_{i}\right)}\ 1_{\left(\overline{T}_i<\overline{T}_j\right)}\equiv Q_d(\overline{T}_{i})^{1/\eta_{i}}\ \Delta(\varepsilon_{i},\eta_{i},\mu_{i},\sigma_{i},\overline{T}_{i},j),$$

$$\begin{aligned}\overline{L}(\overline{T}_i) &= \mathbb{E}^{\mathrm{Q}}_{\overline{T}_i}\int_{\overline{T}_{i-}}^{\infty}\widehat{\pi}*(Q_d(s),\ \boldsymbol{A})\ \mathrm{e}^{-r(s-\overline{T}_{i-})}\ ds-\sum_{\infty}^{j=1}\mathbb{E}^{\mathrm{Q}}_{\overline{T}_{i-}}\left(\widehat{\pi}^*\left(\widetilde{T}_{j-}\right)-\widehat{\pi}^*\left(\widetilde{T}_j\right)\right)\ \mathrm{e}^{-r\left(\tilde{T}_j-\overline{T}_{i-}\right)}\ 1_{\left(\overline{T}_i<\tilde{T}_j\right)}\\ &\quad-\left(\mathbb{E}^{\mathrm{Q}}_{\overline{T}_i}\int_{\overline{T}_{i-}}^{\infty}\widehat{\pi}*(Q_d(s),\ \boldsymbol{A})\ \mathrm{e}^{-r(s-\overline{T}_i)}\ ds-\sum_{\infty}^{j=1}\mathbb{E}^{\mathrm{Q}}_{\overline{T}_i}\ \left(\widehat{\pi}^*\left(\widetilde{T}_{j-}\right)-\widehat{\pi}^*\left(\widetilde{T}_j\right)\right)\ \mathrm{e}^{-r\left(\tilde{T}_j-\overline{T}_i\right)}\ 1_{\left(\overline{T}_i<\tilde{T}_j\right)}\right)\\ &=Q_d(\overline{T}_{i-})^{1/\eta_{i-1}}\ \Upsilon(\varepsilon_{i-1},\eta_{i-1},\mu_{i-1},\sigma_{i-1},\overline{T}_{i-})-Q_d(\overline{T}_i)^{1/\eta_i}\ \Upsilon(\varepsilon_i,\eta_i,\mu_i,\sigma_i,\overline{T}_i)\end{aligned}$$

The explicit forms of the composite functions $\Xi(\cdot)$, $\xi(\cdot)$, $\Delta(\cdot)$, and $\Upsilon(\cdot)$ are all available in Theorems 2 and 3.

The expectation of compensation for i^{th} type-II cyber loss $\mathbb{E}^{\mathrm{Q}}_0\ \phi\ \overline{L}(\overline{T}_i)\mathrm{e}^{-r\overline{T}_i}\ 1_{(\overline{T}_i\le T)}$ thus can be rewritten as (note $\mathbb{E}^{\mathrm{Q}}_0\ \phi\ \overline{L}(\overline{T}_i)\mathrm{e}^{-r\overline{T}_i}\ 1_{(\overline{T}_i\le T)}\equiv\overline{V}(i)$):

$$\begin{aligned}\overline{V}(i)&=\mathbb{E}^{\mathrm{Q}}_0\ \left[\phi\ \left(Q_d(\overline{T}_{i-})^{1/\eta_{i-1}}\ \Upsilon(\varepsilon_{i-1},\eta_{i-1},\mu_{i-1},\sigma_{i-1},\overline{T}_{i-})-Q_d(\overline{T}_i)^{1/\eta_i}\ \Upsilon(\varepsilon_i,\eta_i,\mu_i,\sigma_i,\overline{T}_i)\right)\right.\\ &\quad\left.\times\mathrm{e}^{-rT_i}\ 1_{(T_i\le T)}\right].\end{aligned}$$

Similar to the derivation in Appendix B, repeatedly using Tower law further yields:

$$\begin{aligned}\overline{V}(i)=\mathbb{E}^{Q}_0\Bigg[\ \phi\ \Bigg(&\boldsymbol{Q}^{1/\eta_{i-1}}\ \mathrm{e}^{\xi(\eta_{i-1},\mu_{i-1},\sigma_{i-1},\overline{T}_{i-1},\overline{T}_{i-})+\sum_{i-1}^{k=1}\xi(\eta_{i-1},\mu_{k-1},\sigma_{k-1},\overline{T}_{k-1},\overline{T}_k)}\ \Upsilon(\varepsilon_{i-1},\eta_{i-1},\mu_{i-1},\sigma_{i-1},\overline{T}_{i-})\\ &-\boldsymbol{Q}^{1/\eta_i}\ \mathrm{e}^{\sum_i^{k=1}\xi(\eta_i,\mu_{k-1},\sigma_{k-1},\overline{T}_{k-1},\overline{T}_k)}\ \Upsilon(\varepsilon_i,\eta_i,\mu_i,\sigma_i,\overline{T}_i)\Bigg)\ \mathrm{e}^{-rT_i}\ 1_{(T_i\le T)}\ \Bigg]\end{aligned}$$

and

$$\begin{aligned}\overline{V}(i)=\int_0^T\int_{t_1}^T\cdots\int_{t_{t-1}}^T\Bigg(&\boldsymbol{Q}^{1/\eta_{i-1}}\ \mathrm{e}^{\xi(\eta_{i-1},\mu_{i-1},\sigma_{i-1},t_{i-1},t_{i-})+\sum_{i-1}^{k=1}\xi(\eta_{i-1},\mu_{k-1},\sigma_{k-1},t_{k-1},t_k)}\ \Upsilon(\varepsilon_{i-1},\eta_{i-1},\mu_{i-1},\sigma_{i-1},t_{i-})\\ &-\boldsymbol{Q}^{1/\eta_i}\ \mathrm{e}^{\sum_i^{k=1}\xi(\eta_i,\mu_{k-1},\sigma_{k-1},t_{k-1},t_k)}\ \Upsilon(\varepsilon_i,\eta_i,\mu_i,\sigma_i,t_i)\Bigg)\ \phi\ \mathrm{e}^{-rt_i}\ \prod_{n=1}^{i}\overline{f}_n(t_n)\ dt_i\cdots dt_2\ dt_1\end{aligned}$$

According to the results above, we can summarize the generalized formula as:

$$\begin{aligned}\overline{V}(1)=\int_0^T\ (&\boldsymbol{Q}^{1/\eta_0}\ \mathrm{e}^{\xi(\eta_0,\mu_0,\sigma_0,0,t_{1-})}\ \Upsilon(\varepsilon_0,\eta_0,\mu_0,\sigma_0,t_{1-})\\ &-\boldsymbol{Q}^{1/\eta_1}\ \mathrm{e}^{\xi(\eta_1,\mu_0,\sigma_0,0,t_1)}\ \Upsilon(\varepsilon_1,\eta_1,\mu_1,\sigma_1,t_1))\ \phi\ \mathrm{e}^{-r\ t_1}\ \ \overline{f}_1(t_1)\ dt_1;\end{aligned}$$

$$\begin{aligned}\overline{V}(2)=\int_0^T\int_{t_1}^T\phi\ \mathrm{e}^{-r\ t_2}\ \ (&\boldsymbol{Q}^{1/\eta_1}\mathrm{e}^{\xi(\eta_1,\mu_1,\sigma_1,t_1,t_{2-})+\xi(\eta_1,\mu_0,\sigma_0,0,t_1)}\ \Upsilon(\varepsilon_1,\eta_1,\mu_1,\sigma_1,t_{2-})\\ &-\boldsymbol{Q}^{1/\eta_2}\ \mathrm{e}^{\xi(\eta_2,\mu_0,\sigma_0,0,t_1)+\xi(\eta_2,\mu_1,\sigma_1,t_1,t_2)}\ \Upsilon(\varepsilon_2,\eta_2,\mu_2,\sigma_2,t_2))\ \overline{f}_2(t_2)\ \overline{f}_1(t_1)\ dt_2\ dt_1;\end{aligned}$$

and

$$\begin{aligned}\overline{V}(i)=\int_0^T\int_{t_1}^T\cdots\int_{t_{i-1}}^T\Bigg(&\boldsymbol{Q}^{1/\eta_{i-1}}\ \mathrm{e}^{\xi(\eta_{i-1},\mu_{i-1},\sigma_{i-1},t_{i-1},t_{i-})+\sum_{k=1}^{i=1}\xi(\eta_{i-1},\mu_{k-1},\sigma_{k-1},t_{k-1},t_k)}\ \Upsilon(\varepsilon_{i-1},\eta_{i-1},\mu_{i-1},\sigma_{i-1},t_{i-})\\ &-\boldsymbol{Q}^{1/\eta_i}\ \mathrm{e}^{\sum_{k=1}^{i}\xi\ (\eta_i,\mu_{k-1},\sigma_{k-1},t_{k-1},t_k)}\ \Upsilon(\varepsilon_i,\eta_i,\mu_i,\sigma_i,t_i)\Bigg)\ \phi\ \mathrm{e}^{-rt_i}\ \prod_{n=1}^{i}\overline{f}_n(t_n)\ dt_i\cdots dt_2\ dt_1.\end{aligned}$$

This provides the formula for $\bar{I}(0)=\sum_{i=\bar{L}}^{\overline{U}-1}\ \overline{V}(i)$ and completes the proof.

Appendix D. Elasticity of Sales Revenue to the Markup Pricing Rate

According to Theorem 1 and expressions (2)-(3), we express sales revenue and production costs under the market-cleaning condition below (time arguments are omitted for brevity):

$(p^*)^{1-\varepsilon_i}\ Q_d$ and $\left((p^*)^{-\varepsilon_i}\ Q_d\ \boldsymbol{A}^{-1}\right)^{1/\gamma}\delta.$

Then the markup pricing rate (defined as the ratio of sales revenue to production costs) under optimal product pricing is given by

$$\widetilde{p}^*\equiv\frac{(p^*)^{1-\varepsilon_i}\ Q_d}{\left((p^*)^{-\varepsilon_i}\ Q_d\ \boldsymbol{A}^{-1}\right)^{1/\gamma}\ \delta}=(p^*)^{1-\varepsilon_i+\varepsilon_i/\gamma}\ Q_d^{\,1\ -1/\gamma}\ \boldsymbol{A}^{1/\gamma}\ \ \delta^{\,-1}$$

By using the above expression and applying the chain rule, we derive the unconditional elasticity of sales revenue to the markup pricing rate as follows:

$$\begin{aligned}\xi_{all}(i) &\equiv \frac{d(p^*)^{1-\varepsilon_i}Q_d}{d\widetilde{p}^*}\times\frac{\widetilde{p}^*}{(p^*)^{1-\varepsilon_i}Q_d}\\ &=\frac{\partial(p^*)^{1-\varepsilon_i}Q_d}{\partial p^*}\times\frac{\partial p^*}{\partial\widetilde{p}^*}\times\frac{\widetilde{p}^*}{(p^*)^{1-\varepsilon_i}Q_d}\\ &+\frac{\partial(p^*)^{1-\varepsilon_i}Q_d}{\partial Q_d}\times\frac{\partial Q_d}{\partial\widetilde{p}^*}\times\frac{\widetilde{p}^*}{(p^*)^{1-\varepsilon_i}Q_d}\\ &+\frac{\partial(p^*)^{1-\varepsilon_i}Q_d}{\partial\varepsilon_i}\times\frac{\partial\varepsilon_i}{\partial\widetilde{p}^*}\times\frac{\widetilde{p}^*}{(p^*)^{1-\varepsilon_i}Q_d}\equiv\mathbb{A}+\mathbb{B}+\mathbb{C}\end{aligned}$$

where

$$\begin{aligned}\mathbb{A}=\frac{\partial\ (p*)^{1-\varepsilon_i}\ Q_d}{\partial\ p*}\times p*\times\frac{\partial\ p*}{\partial\ \widetilde{p}*}\times\frac{\widetilde{p}*/p*}{(p*)^{1-\varepsilon_i}\ Q_d}=\frac{\partial\ (p*)^{1-\varepsilon_i}\ Q_d}{\partial\ p*}\times\frac{p*}{(p*)^{1-\varepsilon_i}\ Q_d}\times\frac{\partial\ p*}{\partial\ \widetilde{p}*}\times\frac{\widetilde{p}*}{p*}\\ =\frac{1-\varepsilon_i}{1-\varepsilon_i+\varepsilon_i\ \gamma^{-1}};\end{aligned}$$

$$\begin{aligned}\mathbb{B}=\frac{\partial\ (p*)^{1-\varepsilon_i}\ Q_d}{\partial\ Q_d}\times Q_d\times\frac{\partial\ Q_d}{\partial\ \widetilde{p}*}\times\frac{\widetilde{p}*/Q_d}{(p*)^{1-\varepsilon_i}\ Q_d}=\frac{\partial\ (p*)^{1-\varepsilon_i}\ Q_d}{\partial\ Q_d}\times\frac{Q_d}{(p*)^{1-\varepsilon_i}\ Q_d}\times\frac{\partial\ Q_d}{\partial\ \widetilde{p}*}\times\frac{\widetilde{p}*}{Q_d}\\ =\frac{1}{1-\gamma^{-1}}\end{aligned}$$

and $\mathbb{C}=\frac{\partial\ (p*)^{1-\varepsilon_i}\ Q_d}{\partial\ \varepsilon_i}\times\frac{\partial\ \varepsilon_i}{\partial\ \widetilde{p*}}\times\frac{\widetilde{p*}}{(p*)^{1-\varepsilon_i}\ Q_d}=\frac{-1}{\gamma^{-1}-1}$, because $\frac{\partial\ (p*)^{1-\varepsilon_i}\ Q_d}{\partial\ \varepsilon_i}=-(p*)^{1-\varepsilon_i}\ Q_d\ lnp*$. and $\frac{\partial\ \varepsilon_i}{\partial\ \widetilde{p*}}=(\widetilde{p}*)^{-1}\ \left(\gamma^{-1}-1\right)^{-1}\ (\ln p*)^{-1}$.

Hence, we yield the explicit form of the unconditional elasticity of sales revenue:

$$\xi_{all}(i)=\frac{1}{1-\gamma^{-1}+\frac{\gamma^{-1}}{1-\varepsilon_i}}+\frac{2}{1-\gamma^{-1}}=\frac{1}{1-\gamma^{-1}+\frac{\gamma^{-1}}{1-\varepsilon_L-(\varepsilon_U-\varepsilon_L)(1-\varpi)^{\ i}}}+\frac{2}{1-\gamma^{-1}},$$

where i denotes the number of type-II cyber event occurrences. Changes in the state of this number do not affect the structure of sales revenue and the markup pricing rate. Consequently, the elasticity of sales revenue in the data-breach-free scenario takes a corresponding form:

$$\xi_{pre}=\xi_{al}(0)=\frac{1}{1-\gamma^{-1}+\frac{\gamma^{-1}}{1-\varepsilon_U}}+\frac{2}{1-\gamma^{-1}}.$$

This completes the proof.

Data availability

The authors do not have permission to share data.

References

Baione, F., Levantesi, S., 2014. A health insurance pricing model based on pre-valence rates: application to critical illness insurance. Insur.: Math. Econ. 58, 174–184.

Biagini, F., Groll, A., Widenmann, J., 2013. Intensity-based premium evaluation for Unemp-loyment Insurance products. Insur.: Math. Econ. 53, 302–316.

Biener, C., Eling, M., Wirfs, J.H., 2015. Insurability of cyber risk: an empirical analysis. Geneva Pap. Risk Insur. Issues Pract. 40, 131–158.

Böhme, R., Kataria, G., 2006. Models and Measures for Correlation in Cyber Insurance, working paper. Technische Universität Dresden.

Braun, A., Eling, M., Jaenicke, C., 2023. Cyber insurance-linked securities. ASTIN Bull. 53, 1–22.

Caballero, R., Engel, E., 1999. Explaining investment dynamics in U.S. Manufacturing: A generalized (S,s) approach. Econometrica 67, 783–826.

Cao, X., Ni, J., Wang, F., Xu, Y., 2023. Does customer concentration affect corporate risk-taking? Evidence from China. Finance Res. Lett. 58, 104297.

Chang, C., Lin, S., Yu, M., 2011. Valuation of catastrophe equity puts with Markov-modulated poisson processes. J. Risk Insur. 78 (2), 447–473.

Chang, C., Wang, C.W., Yang, C.Y., 2012. The effects of macroeconomic factors on pricing mortgage insurance contracts. J. Risk Insur. 79, 867–895.

Chang, T.Z., Wildt, A., 1994. Price, product information, and purchase intention: an empirical study. J. Acad. Mark. Sci. 22, 16–27.

Chen, J., Su, X., Tian, X., Xu, B., 2022. Does customer-base structure influence managerial risk-taking incentives? J financ econ 143, 462–483.

Chen, C., Chang, C., 2019. How big are the ambiguity-based premiums on mortgage insurances? J. Real Estate Finance Econ. 58, 133–157.

Chen, C., Chang, C., Sun, E.W., Yu, M., 2022. Optimal decision of dynamic wealth allocation with life insurance for mitigating health risk under market incompleteness. Eur J Oper Res 300 (2), 727–742.

Chong, W.F., Feng, R., Hu, H., Zhang, L., 2023. Cyber Risk Assessment for Capital Management. Tsinghua University, Cornell University, The Ohio State University working paper.

Chuang, H., Yu, M., 2010. Pricing unemployment insurance - an unemployment-duration-adjusted approach. ASTIN Bull. 40, 519–545.

Doerrenberg, P., Peichl, A., Siegloch, S., 2017. The elasticity of taxable income in the presence of deduction possibilities. J Public Econ 151, 41–55.

Duan, J.C., Yu, M., 1999. Capital standard, forbearance, and Deposit Insurance coverage under GARCH. J. Bank. Finance 23, 1691–1706.

Duan, J.C., Yu, M., 2005. Fair insurance guaranty Premia in the presence of risk-based capital regulations, stochastic interest rates, and catastrophe risk. J. Bank. Finance 29, 2435–2454.

Dynes, S., Johnson, M.E., Andrijcic, E., Horowitz, B., 2007. Economic costs of firm-level information infrastructure failures: estimates from field studies in manufacturing supply chains. Int. J. Logist. Manag. 18, 420–442.

Eling, M., Jung, K., 2018. Copula approaches for modeling cross-sectional dependence of data breach losses. Insur.: Math. Econ. 82, 167–180.

Eling, M., Schnell, W., 2016. What do we know about cyber risk and cyber risk insurance? J. Risk Finance 17, 474–491.

Eling, M., Schnell, W., 2020. Capital Requirements for Cyber risk and Cyber risk insurance: an analysis of Solvency II, the U.S. Risk-based Capital standards, and the Swiss Solvency Test. N. Am. Actuar. J. 370–392.

Eling, M., Wirfs, J., 2019. What are the actual costs of cyber risk events? Eur J Oper Res 272, 1109–1119.

Fahrenwaldt, M., Weber, S., Weske, K., 2018. Pricing of cyber insurance contract in A network model. ASTIN Bull. 48, 1175–1218.

Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V., Gordon, L., Wang, S., Schmit, J., Thomas, R., Elvedi, M., Maillart, T., Donavan, E., Dejung, S., Durand, E., Nutter, F., Scheffer, U., Arazi, G., Ohana, G., Lin, H., 2019. Cyber risk research impeded by disciplinary barriers. Science 366, 1066–1069.

Fischer, T., 2007. A law of large numbers approach to valuation in life insurance. Insur.: Math. Econ. 40, 35–57.

Franke, U., 2017. The Cyber insurance market in Sweden. Comput. Secur. 68, 130–144.

Garrison, C.P., Ncube, M., 2011. A longitudinal analysis of data breaches. Inf. Manag. Comput. Secur. 19, 216–230.

Goldstein, R., Ju, N., Leland, H., 2001. An EBIT-based model of dynamic capital structure. J. Bus. 74, 483–512.

Gordon, L.A., Loeb, M.P., Sohail, T., 2003. A framework for using insurance for Cyber risk management. Commun ACM 46, 81–85.

Gupta, S., Lehmann, D.R., 2003. Customers as assets. J. Interact. Mark. 17, 9–24.

Gupta, S., Lehmann, D.R., Stuart, J.A., 2004. Valuing customers. J. Mark. Res. 41, 7–18.

Herath, H., Herath, T.C., 2007. Cyber Insurance: Copula Pricing Framework and Implications for Risk Management. Brock University working paper.

Herath, H., Herath, T.C., 2011. Copula based actuarial model for pricing cyber-insurance policies. Insur. Mark. Co.: Anal. Actuar. Comput. 2, 7–20.

Janakiraman, R., Lim, J.H., Rishika, R., 2018. The effect of a data breach announcement on customer behavior: evidence from a multichannel retailer. J Mark 82, 85–105.

Kalyanaram, G., Winer, R., 1995. Empirical generalizations from Reference Price Research. Mark. Sci. 14, 161–169.

Kamiya, S., Kang, J., Kim, J., Milidonis, A., Stulz, R., 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. J financ econ 139, 719–749.

Kelic, A., Collier, Z.A., Brown, C., Beyeler, W.E., Outkin, A.V., Vargas, V.N., Ehlen, C., Zaidi, A., Leung, B., Linkov, I., 2013. Decision framework for evaluating the macroeconomic risks and policy impacts of cyber attacks. Environ. Syst. Decis. 33, 544–560.

Lee, J.P., Yu, M., 2007. Valuation of catastrophe reinsurance with CAT bonds. Insur.: Math. Econ. 41, 264–278.

Low, W.S., Lee, J.D., Cheng, S.M., 2013. The link between customer satisfaction and price sensitivity: an investigation of retailing industry in Taiwan. J. Retail. Consum. Serv. 20, 1–10.

McAfee, 2014. Net Losses: Estimating the Global Cost of Cybercrime.

Miao, J., 2005. Optimal capital structure and industry dynamics. J. Finance 60, 2621–2659.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A., Sadhukhan, S.K., 2013. Cyber-risk decision models: to insure IT or not? Decis Support Syst 56, 11–26.

Mukhopadhyay, A., Saha, D., Mahanti, A., Podder, A., 2005. Insurance for cyber risk: A utility model. Decision 32, 153–170.

Neisser, C., 2021. The elasticity of taxable income: A meta-regression analysis. Econ. J. 131, 3365–3391.

PCI Pal, 2019. This is the World: The State of Security in the Eyes of Consumers.

Ponemon Institute, 2016. The Cost of Cyber Crime and the Role of Information Management.

Su, K.C., Lee, C.B., Lin, S.H., Liu, I.C., Chen, H.C., 2021. Pricing cyber risk: the copula-based approach. Adv. Pac. Basin Bus. Econ. Finance 9, 161–174.

Symantec Corporation, 2013. Internet Security Threat Report.

Wagner, S., Bode, C., 2008. An empirical examination of supply chain performance along several dimensions of risk. J. Bus. Logist. 29, 307–325.

Wang, S., 2019. Integrated framework for Information Security investment and Cyber insurance. Pac.-Basin Finance J. 57, 1–12.

Xu, M., Hua, L., 2019. Cybersecurity insurance: modeling and pricing. N. Am. Actuar. J. 23, 220–249.

Yang, S.Y., Wang, C.W., Huang, H.C., 2016. The valuation of lifetime health insurance policies with limited coverage. J. Risk Insur. 83, 777–800.

Young, V.R., 2008. Pricing life insurance under stochastic mortality via the instantaneous sharpe ratio. Insur.: Math. Econ. 42, 691–703.