Computers & Security 157 (2025) 104585

Contents lists available at ScienceDirect

Computers & Security

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

Full length article

To insure or not to insure: How attackers exploit cyber-insurance via game theory

Zhen Li [a], Qi Liao [b,*]

[a] Department of Economics & Management, Albion College, USA
[b] Department of Computer Science, Central Michigan University, USA

ARTICLE INFO

Keywords:
Cybersecurity
Cyber-insurance
Game theory
Attacker
Manipulation and exploitation
Best strategies
Cybersecurity investment
Cybersecurity portfolio management
Optimization

ABSTRACT

Cyber-insurance provides organizations with financial protection against losses from cyber incidents. As its adoption grows, organizations face the challenge of balancing investments in cybersecurity defense measures with the acquisition of cyber-insurance. This convergence presents opportunities but also introduces risks. The effects of cyber-insurance on the interplay between cybersecurity investment and attacker strategies remains poorly understood. In this paper, we systematically analyze an organization's decision-making process regarding optimal cybersecurity investment and cyber-insurance, with a particular focus on the strategic behavior of attackers. Using economic and game-theoretic models, supported by simulation studies, our findings reveal that while cyber-insurance can mitigate financial losses, it may inadvertently weaken overall cybersecurity defenses. Furthermore, we demonstrate that cyber-attacks are not random events but calculated actions influenced by the attacker's understanding of the organization's insurance and defense posture. Attackers can exploit cyber-insurance by strategically launching targeted attacks to manipulate an organization's reliance on insurance and disrupt its investment equilibrium. This manipulation can persist up to a critical threshold, beyond which escalating threats prompt organizations to strengthen their defenses. In this way, attackers effectively "play God," strategically shaping an organization's insurance and cybersecurity portfolio. To counter these risks, we propose actionable recommendations to prevent attackers from exploiting the cyber-insurance market, ensuring a more resilient and secure cybersecurity ecosystem.

1. Introduction

Computer-based information systems have increased the efficiency of organizational operations but also changed the way organizations view cybersecurity. Digital revolution creates risks of actual and potential cybersecurity breaches. It is easy to see how cyber attacks can be financially devastating for organizations, often forcing them to shutter their operations. Numerous empirical studies point out the adverse effect cyber breaches have on the performance of organizations in nearly every industry dealing with cyber risk on a daily basis, and the financial devastation of cyber-attacks is only growing (Aldasoro et al., 2022; Eisenbach et al., 2021; Kamiya et al., 2018). The cybersecurity risks and incidents confronting organizations provide incentives for organizations to invest in cybersecurity. While cybersecurity investment provides preventive cybersecurity measures such as firewalls, intrusion prevention systems and business continuity and disaster recovery mechanisms, cyber-insurance provides cybersecurity coverage and financial security against damage arising out of a cyber event, specifically designed to address data-breach-related expenses including forensic investigations and monetary losses. Since cyber-insurance started in the mid to late 1990s, the number of organizations choosing cyber-insurance has been rising (Baker and Shortland, 2023).

Cyber-insurance is an insurance policy that assists in the timely recovery from cyber attacks and incidents. Coverage may include the liability of lost data, the damage to technology assets, the cost of business disruptions, informing affected clients, paying ransoms, and expenses and costs associated with legal issues. Like any insurance product, cyber-insurance pools the risks of cyber-attacks among policyholders. While cyber-insurance does not fundamentally change the overall destruction that a cybersecurity incident can cause, it reduces the organization's out-of-pocket payment ("private loss") in case of such an incident. In other words, cyber-insurance is to mitigate the organization's financial risk exposure in the aftermath. Meanwhile, like any insurance product, cyber-insurance is subject to moral hazard. When cyber-insurance policyholders know the insurers will pay for their losses, they in turn act in a riskier way, increasing the chance of

* Corresponding author.
E-mail address: liao1q@cmich.edu (Q. Liao).

https://doi.org/10.1016/j.cose.2025.104585
Received 15 March 2025; Accepted 26 June 2025
Available online 9 July 2025

cyber incident. In addition, cyber-insurance may generate direct payments to the attacker, especially for ransomware attacks. Ransomware is one of the top cyber threats driving organizations to buy cyber-insurance (Tsohou et al., 2023). That is, cyber-insurance may increase not only the attack success rate, but also the chance of receiving payoffs from a successful attack, as in ransomware case.

Cyber-insurance is still a new concept in practice and research with many open questions regarding the data and economic models driving it, the coverage options, premium pricing, and the more procedural policy-related aspects. In particular, its effects on cybersecurity remain ambiguous. Unlike the established insurances (e.g., home, auto, health, etc.) where the odds of incidents are more of "act of God" (e.g., a lightening hitting a house), in the new cyber-insurance, the odds of cyber incidents are more controllable by the attacker. In some sense, the attacker's action is like the "hand of God" that controls the chance of cyber incidents. Therefore, studying cyber-insurance without considering the attacker's reactions to cyber-insurance is missing an essential aspect of the situation.

This research pays special attention to the attacker's perspective and asks questions such as "Is cyber-insurance really good for cybersecurity?", "Does cyber-insurance benefit the insured or the attacker?", "Can attackers benefit from the practice of cyber-insurance?", etc. By modeling a game between the attacker and the organization, we study the optimal strategies of both parties.

The novelty of this research is to study the possibility of attackers' manipulation of cyber-insurance in their own favor by measuring the optimal cybersecurity investment level of the organization with and without cyber-insurance. A key determinant is the cyber threat imposed on the organization by the attacker. The attacker's action affects the organization's incentives to acquire cyber-insurance. Depending on how cyber-insurance affects the attacker's benefits, the attacker strategically chooses attack probability imposing on the organization.

The modeling analysis suggests a decrease in the organization's optimal cybersecurity investment with cyber-insurance, and there is a significant increase in the attacker's expected payoff as the organization shifts from no cyber-insurance to cyber-insurance. Beyond that point of switch, imposing further threat on the organization will force the organization to invest more in cybersecurity. In this scenario, the best response of the attacker is to impose just the right amount of cyber threat to "induce" the organization to purchase cyber-insurance. One of our important contributions is the finding of the critical point of attack probability for the organization's switching to cyber-insurance therefore significantly increasing attack payoff. To the best of our knowledge, this is the first study of the implications of cyber-insurance on the benefits of attackers per se and attackers' potential to manipulate the mechanism to serve their own best interest. Plausible countermeasures against the potential manipulation are then discussed.

This research studies also the composition of the organization's expenditure on cybersecurity and how it may react to the attacker's actions. When the organization invests in cybersecurity infrastructure and/or acquires cyber-insurance coverage, it is both due to the common concern about the risk of a data breach or a technology disruption caused by malicious cyber attacks. While cybersecurity investment provides preventive cybersecurity measures, having cyber-insurance coverage provides contingent coverage when bad things happen. Without purchasing cyber coverage, the breached organization would have to pay for all the losses. The organization has incentives to invest in cybersecurity. Cyber-insurance serves as indirect investment in cybersecurity, i.e., instead of investing in preventive technologies, the organization spends on cyber-insurance premium to be covered. With cyber-insurance, the organization is given the chance to compile a cyber risk management package composed of both cybersecurity investment and cyber-insurance, referred to as a "cybersecurity portfolio". We illustrate with case study the organization's relevant decision-making in various scenarios.

The rest of the paper is organized as follows. Section 2 reviews related literature on cyber-insurance. Section 3 constructs an economic model to derive the organization's optimal level of cybersecurity investment without and with cyber-insurance. Section 4 conducts a game-theoretic analysis of the interactions between the organization and the cyber attacker to derive the optimal choices of the two game players without and with cyber-insurance. A plausible game solution is derived focusing on the attacker's probability of launching attacks and potential manipulation of cyber-insurance. Section 5 discusses various factors and measures that may alleviate the attacker's manipulation of cyber-insurance. Section 6 goes through numerical examples demonstrating the model implications and the organization's various decision-making. Finally, Section 7 concludes the work and discusses future research.

2. Related work

Compared to established lines of insurance services, cyber-insurance is at its early stage of development and is particularly complicated as it has to tackle with complex challenges and obstacles such as the uncertainty generated by diversity of insurance coverage (Woods and Böhme, 2021; Panda et al., 2019). There are concerns about the insurance coverage, lack of information, and the complexity of the cyber-related claims (Bandyopadhyay and Mookerjee, 2019). With malicious users present, equilibrium cyber-insurance contracts that specify user security fail to exist, and thus cyber-insurers fail to underwrite contracts conditioning the premiums on security in a general setting (Galina et al., 2013). Nevertheless, there is an increasing demand for cyber-insurance and the market has been growing rapidly. Cyber-insurance has existed since the late 1990s (Böhme et al., 2018). Without considering catastrophic scenarios, the vast majority of cyber risks is insurable and cyber-insurance can be profitable (Kesan et al., 2005; Pal et al., 2018, 2011). Post-incident covering by cyber-insurance contracts is commonly seen (Tsohou et al., 2023). The insurers may offer not only cyber-insurance contracts but also risk management services (Talesh, 2018). Along with the rising industry is a rapidly increasing body of research addressing cyber-insurance. Surveys and literature reviews offer overviews that classify cyber-insurance research into various areas, identifying and categorizing practical and research problems and cyber-insurance challenges, providing the landscape and trends of the research, and proposing possible solutions (Dambra et al., 2020; Tsohou et al., 2023; Aziz et al., 2020).

Cyber-insurance appears to be a viable method for cyber risk transfer. A three-player game (Tosh et al., 2017) implies that attacks motivate the organization to consider cyber-insurance option for transferring the risks. It is generally agreed that cyber-insurance is effective at post-incident responses (Talesh, 2018; Nurse et al., 2020), but numerous problems with the insurability of cyber risks persist that impede the further development of the cyber-insurance market. Cyber-insurance is subject to the general problems of adverse selection and moral hazard prevailing insurance markets (Ehrlich and Becker, 1972). Information asymmetries hinder cyber risk management via cyber-insurance (Laszka et al., 2018; Bandyopadhyay et al., 2009). Moral hazard, or the reactive nature of insured risk, is present to varying degrees whenever there is insurance (Baker, 1996). Cyber insurance facilitates organizations by providing financial resources and expertise when a cyber incident occurs and, sometimes, by providing loss prevention advice in advance. Nevertheless, recent research reveals that the insured tends not to take advantage of cyber insurers' loss prevention services, except in the context of recovering from a breach (Cunningham and Talesh, 2021; Baker and Shortland, 2023).

The moral hazard problem of cyber-insurance also includes the so-called "third party moral hazard", defined as the influence of insurance on the loss-creation or claiming behavior of uninsured third parties, i.e., non-parties to the insurance contract (Parchomovsky and Siegelman, 2022). The presence of cyber-insurance can create an incentive for

loss-creation by attackers who are not party to the insurance contract – but potentially knowledgeable about – the insurance contract, presenting a third-party moral hazard that is hard to control (Parchomovsky and Siegelman, 2022). The attacker is capable of manipulating the attack probability to influence the organization's incentives of purchasing cyber-insurance (Li and Liao, 2023). Insurance against cyber-ransoms has been linked to an increase in attacks by funding and expediting ransom payments that encourages further attacks (Baker and Shortland, 2023; Cartwright et al., 2023; Wolff, 2022), and ransomware has been a key cause for the insurers to revise their business models (Mott et al., 2023).

The effects of cyber-insurance on cybersecurity investment is an open question. Cyber-insurance could result in higher cybersecurity investment depending on the insurers' ability to deal with potential adverse selection, moral hazard, and other problems in the cyber-insurance market (Kesan et al., 2005). An insurance contract incentivizing the insured to adopt preventative measures and implement best practices can improve cybersecurity provided by premium discrimination and the design of customized policies (Hayel and Zhu, 2015; Khalili et al., 2018; Uuganbayar et al., 2021). Security interdependence affects the incentive of users to invest in self-protection with and without cyber-insurance (Uuganbayar et al., 2018). As for the amount of self-defense investments users spend in networked environments with externalities, cyber-insurance is an incentive to self-defense investments only if the quality of self-defense is not very good, and the initial security level of a user is poor (Yang and Lui, 2014). Cooperation amongst network users will result in a more robust cyberspace (Pal and Golubchik, 2010). The key to improving overall network security lies in incentivizing users to invest in sufficient self-defense investments despite of the possible free-riding on others' investing in the network. Under conditions of no information asymmetry between the insurer and the insured, cyber-insurance incentivizes users to invest in self-defense (Bolot and Lelarge, 2008; Lelarge and Bolot, 2009).

Recent empirical evidence though, suggests that today's cyber-insurance market is not effectively exercising predicted governance functions on cybersecurity (Woods and Moore, 2020). Depending on the features of the underlying environment, cyber-insurance may or may not improve the state of network security (Uuganbayar et al., 2018). In a model where a user's probability to incur cyber damage depends on both private security and network security, competitive cyber-insurers may fail to improve network security (Shetty et al., 2010). Modeling the reactivity of the attacker to cybersecurity investment as an endogenous risk generating mechanism, it was shown that cyber-insurance may have negative effects on security investment (Massaccia et al., 2017). Without contract discrimination, the cyber-insurance market equilibrium is inefficient and does not increase cybersecurity (Pal et al., 2014; Khalili et al., 2018, 2019). There is little empirical evidence that cyber-insurance gives motives for the insured to invest in cybersecurity (Wolff, 2022; Talesh and Cunningham, 2021). A big challenge is the insurers' missing solid methodologies, standards, and tools to carry out their measurements, assessing the level of cybersecurity controls and related risk (Romanosky et al., 2019). Unlike traditional insurance that derives the premium from target value and statistical models, an alternative scoring model was proposed for cyber-insurance that is based on the results of internal and external audits and compliance with mandatory and voluntary standards (Piromsopa et al., 2017). A unifying framework was introduced considering interdependent security, correlated risk, and information asymmetries of cyber-insurance to understand the discrepancies (Böhme and Schwartz, 2010). To what extent cyber-insurance companies influence global diffusion of cybersecurity protection and mechanisms is unclear (Woods and Böhme, 2021). To date, the cybersecurity implication of cyber-insurance remains a field of ambiguity.

We extend the Gordon–Loeb (GL) model (Gordon and Loeb, 2002; Gordon et al., 2015) of economic cost-benefit research on cybersecurity investment to show that cyber-insurance may have a negative impact on cybersecurity. Although cyber-insurance is beneficial to the insured from an economic perspective, it is not beneficial from a cybersecurity perspective. We study the incentive mechanisms of cyber-insurance based on the observation that cyber risk is not being random but largely in the control of the attacker. The attacker can intentionally manipulate the system by adjusting attack strategies to influence the organization's decision of purchasing cyber-insurance, gaining from cyber-insurance. Factors and countermeasures that can alleviate the attacker's manipulation of cyber-insurance are explored. The derived insights are applicable regardless of whether cyber-insurance has positive or adverse overall effects on cybersecurity investment.

Table 1
Symbols and Definitions.

Symbol/Variable	Definition
C_s	Cost of additional cybersecurity investment
C_i	Cost of cyber-insurance (premium on cyber-insurance policy)
L_0	Cyber incident loss without cyber-insurance
L_1	Cyber incident loss private to the organization with cyber-insurance
t	Attack probability
r	Attack success rate at existing cybersecurity investment
$R(C_s, r)$	Attack success rate with additional cybersecurity investment
P^a	Attacker's payoff from a successful attack
C^a	Attacker's cost of launching an attack

3. An economic model of cybersecurity investment and cyber-insurance

We first conduct the economic analysis of how an organization forms a cybersecurity portfolio to defend against cyber-attack threats. The cybersecurity portfolio comprises two types of financial investment in cybersecurity: investment in cybersecurity infrastructure (hereinafter referred to as "cybersecurity investment") and investment in cyber-insurance policy (hereinafter referred to as "cyber-insurance"). The key difference between cybersecurity investment and cyber-insurance is that the former is preventive measures affecting the organization's fundamental vulnerability to cyber attacks and the latter is aftermath coverage and clean-up, which by itself, does not affect the inherent cyber vulnerability of the organization.

How much should the organization invest in the cybersecurity portfolio? All in all, the organization is driven by the desire to earn profit, and its decisions are largely the result of the cost–benefit analysis. We apply and extend economic production theory to the problem of assessing the impacts of cybersecurity investment and cyber-insurance. The production theory framework is based on the analysis of the relationship between inputs and output, or equivalently, costs and benefits. The use of cost–benefit analysis for efficiently allocating scarce resources is well established in the capital investment literature including the literature on investment in cybersecurity.

We consider a one-period model of an organization contemplating a cybersecurity portfolio made up of cybersecurity investment and cyber-insurance. The organization is risk-neutral meaning that it is indifferent to amounts of investment or forms of investment as long as they have the same expected net value, regardless of various levels of risk and uncertainty. In comparison, an organization that is risk averse would require a higher expected net value on more risky investment. Table 1 lists the variables used in the model and their brief meanings.

3.1. Input and output of cybersecurity investment

The input of cybersecurity investment includes financial investment used to strengthen cybersecurity systems such as intrusion detection/prevention systems, firewalls, malware detection, antivirus and improved software, one time password tokens, two-factor authentications, encryptions, internal control systems, user education/training

programs, etc. The organization's additional spending on cybersecurity investment is represented by C_s.

The output of cybersecurity investment is gauged by the reduced attack success rate enabled by additional cybersecurity investment. The benchmark model is based on the GL model, a commonly used model to assess optimal security investment at the firm level. In particular, we measure the potential loss of cyber incident using triple variables $\{t, r, L_0\}$ where $t \in [0, 1]$ is the attack probability that the attacker may launch an attack on the organization and L_0 is the overall incident loss of a successful attack. L_0 is finite and less than some very large number for the risk-neutrality assumption to apply. In economic terminology, the disutility of a catastrophic loss is so large that the organization would prefer the expected value of the gamble rather than risking a loss of L_0.

Specifically, $r \in [0, 1]$ is used to denote the attack success rate at existing cybersecurity investment, the probability that without additional cybersecurity investment, a cyber attack will result in the organization's being victim of the attack and the loss L_0 occurring. The organization is completely secure when $t = 0$ or $r = 0$. Typically, the attack probability on the organization and the attack success rate fall in the interior of $0 < t < 1$ and $0 < r < 1$. $t \times r$ is the probability of the loss occurring, i.e., "risk of the loss" of the organization. $t \times r \times L_0$ is the organization's expected loss conditioned on no additional cybersecurity investment in absence of cyber-insurance. The organization's cybersecurity investment decision is on incremental investment spending, based on the implicit assumption that the organization already has some cybersecurity infrastructure in place, resulting in existing current attack success rate. Therefore, there are no incremental fixed costs associated with additional cybersecurity investment, only variable costs.

The expenditure of C_s is to reduce the attack success rate. Let $R(C_s, r)$ be the attack success rate on the organization that has additional cybersecurity investment. $R(C_s, r)$ is continuously twice differentiable. The nature of cyber vulnerability leads to the following features of the R function:

- $R(C_s, 0) = 0$ for all C_s. That is, if the organization is initially perfectly secure, then it will remain perfectly secure with any amount of additional cybersecurity investment.
- $R(0, r) = r$ for all r. That is, if there is no additional cybersecurity investment, the attack success rate remains unchanged at the initial level associated with existing cybersecurity investment.
- $R'(C_s, r) < 0$ and $R''(C_s, r) > 0$ for all $r \in (0, 1)$ where R' and R'' denote the first and second-order partial derivatives of the R function with respect to C_s, respectively. That is, cybersecurity is increasing in cybersecurity investment at a decreasing rate.

3.2. Input and output of cyber-insurance

Cyber-insurance is specifically designed to address cyber-incident-related losses. The organization has to pay a premium to be insured. Due to moral hazard concerns, insurance policies normally come with deductibles. Being insured can significantly reduce the cyber incident loss the organization has to pay out of own pockets (hereinafter referred to as the "incident loss private to the organization", e.g., the deductible).

Whether the organization is cyber-insured or not does not change the total incident loss L_0, nor does it change the attack success rate at a certain cybersecurity investment level, i.e., r and $R(C_s, r)$ are both independent of C_i. The expenditure of C_i is to reduce the organization's private loss in case of an incident. Suppose cyber-insurance reduces the organization's private loss from L_0 to L_1. L_1 includes the deductible and the part of incident loss not covered by cyber-insurance. It can also be extended to include the net present value of expected future increase in cyber-insurance premium.

From above, the input of cyber-insurance is the premium on cyber-insurance policy to have the organization covered, i.e., C_i. The output of cyber-insurance is the reduced incident loss private to the organization under the coverage of cyber-insurance, i.e., $tR(C_s, r)(L_0 - L_1)$ where $tR(C_s, r)$ is the probability of incident occurring.

To decide on additional cybersecurity investment and the purchase of cyber-insurance, the organization compares input and output of the two.

3.3. How much more to invest in cybersecurity infrastructure without cyber-insurance?

We begin with the case when cyber-insurance is not an option yet, i.e., $C_i = 0$. The expected benefit of cybersecurity investment is equal to the reduction in the organization's expected loss attributed to additional cybersecurity investment.

$$[r - R(C_s, r)]tL_0 \tag{1}$$

Since C_s is the cost of additional cybersecurity investment, the expected net benefit of cybersecurity investment is

$$[r - R(C_s, r)]tL_0 - C_s \tag{2}$$

Of variables in (2), t is the control variable of the attacker. r and L_0 are the given parameters specifying the existing status of cybersecurity and vulnerability of the organization. C_s is the only control variable of the organization. The risk-neutral organization's goal is to choose optimal additional cybersecurity investment C_s^* that maximizes (2). C_s^* is found by solving the first-order condition of the objective function (2) with respect to C_s.

$$-R_1(C_s^*, r)tL_0 = 1 \tag{3}$$

where the left-hand-side is the marginal benefit of cybersecurity investment measured by the decrease in the attack success rate when increasing cybersecurity investment by one unit. This partial derivative can be interpreted as the marginal productivity of cybersecurity investment. The right-hand-side is the marginal cost of increasing cybersecurity investment by one unit.

3.4. How much more to invest in cybersecurity infrastructure with cyber-insurance?

When cyber-insurance is an option, the organization makes rational choice to determine if it needs cyber-insurance based on its own risk exposure. The insurer offers various combinations of premium and deductible to the organization, corresponding to the coverage and the attack success rate. The premium, or the price of insurance, is the monetary value for which the organization agrees to exchange risk. It is challenging to price cyber-insurance policies. Classical actuarial approaches, game theoretical approaches, and more complex valuation models have been used in the modeling and pricing of cyber-insurance. For both practitioners and researchers, modeling and pricing cyber-insurance constitutes a relatively new topic that is still in infancy (Awiszus et al., 2023). In the one-period model, we assume the price of purchasing cyber-insurance depends on existing cybersecurity investment but not on the additional cybersecurity investment the organization will choose after purchasing cyber-insurance (which will affect future premium). Hence the organization's choice of cybersecurity investment (after being insured) does not affect the current premium, similar to a driver's current driving habits (after being insured) does not affect the current premium on the auto insurance policy but the future premium.

The premium and the deductible are inversely related. The inverse relationship may apply to the following scenarios:

- The organization chooses a cyber-insurance policy that has a high deductible to reduce the premium, or a high premium to reduce the deductible.

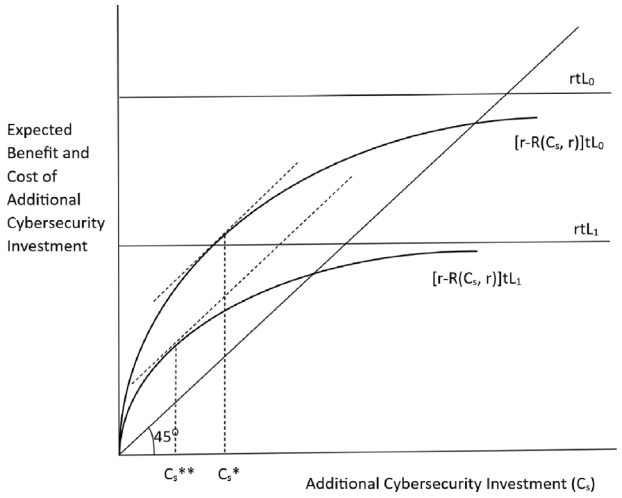


Fig. 1. Optimal additional cybersecurity investment with and without cyber-insurance.

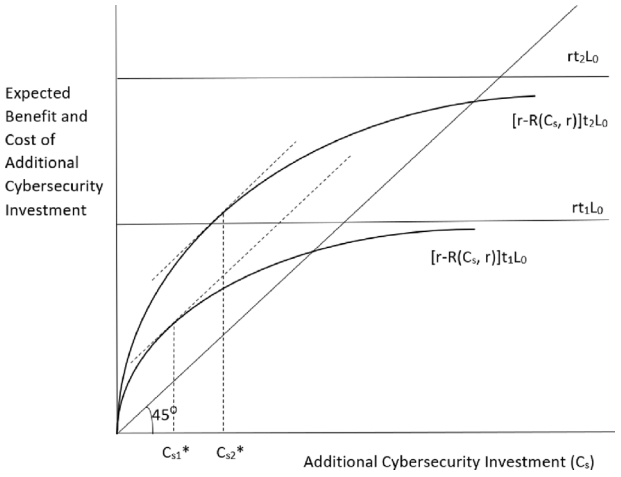


Fig. 2. Effects of attack probability on optimal additional cybersecurity investment.

- The organization pays a high premium on a cyber-insurance policy with broad coverage that reduces the organization's private loss in case of incident.

Cyber-insurance reduces the organization's private loss from L_0 to L_1. L_1 captures the deductible. Taking as given its chosen cyber-insurance package of $\{L_1, C_i\}$, the organization's expected benefit of additional cybersecurity investment with cyber-insurance is

$$[r - R(C_s, r)]tL_1 \tag{4}$$

The expected net benefit of additional cybersecurity investment with cyber-insurance is

$$[r - R(C_s, r)]tL_1 - C_s \tag{5}$$

The organization chooses optimal additional cybersecurity investment, C_s^{**}, to maximize (5):

$$-R'(C_s^{**}, r)tL_1 = 1 \tag{6}$$

3.5. Effects of cyber-insurance on cybersecurity investment

The optimal additional cybersecurity investment changes with the organization's private loss that is different when the organization is insured or not insured.

From (3),

$$-R'(C_s^{*}, r) = \frac{1}{tL_0} \tag{7}$$

From (6),

$$-R'(C_s^{**}, r) = \frac{1}{tL_1} \tag{8}$$

If the organization were perfectly secure ($r = 0$), then no cybersecurity investment would be necessary ($C_s^{*} = C_s^{**} = 0$). At some sufficiently large attack success rate, it would be optimal to make positive additional cybersecurity investment.

Since R' is increasing in C_s and $L_0 > L_1$, optimal additional cybersecurity investment decreases when the organization has cyber-insurance coverage, i.e., $C_s^{**} < C_s^{*}$. The decrease in the organization's choice of additional cybersecurity investment with cyber-insurance is a moral hazard issue in cyber-insurance. In the context of the model, the term "moral hazard" refers to the responsiveness of cybersecurity investment spending to insurance coverage, capturing the notion that insurance coverage, by lowering the marginal cost of cyber incident to the organization, decreases the organization's use of cybersecurity investment.

Fig. 1 illustrates the relative amounts of optimal additional cybersecurity investment. The horizontal axis is the various levels of additional cybersecurity investment. The vertical axis measures the expected benefits and costs of cybersecurity investment with and without cyber-insurance. The concave curves are for (1) and (4), respectively, of which, the lower curve is for (4). Both curves of expected benefits start from the origin at $R(0, r) = r$. They increase at a decreasing rate and converge to rtL_0 and rtL_1, respectively, as $C_s \to \infty$. The 45° line is the cost curve of cybersecurity investment. The vertical distance between the concave benefit curve and the linear cost curve is the expected net benefit, as in (2) and (5), and the additional cybersecurity investment corresponding to the largest distance is optimal. Note the intersection of the expected benefit curve and the cost curve corresponds to the largest feasible additional cybersecurity investment. As long as cybersecurity investment stays below this amount, the organization's expected net benefit is positive. That is, it receives a net gain from additional cybersecurity investment. Nevertheless, the net benefit is maximized at an amount lower than the feasible upper-bound. As shown, the organization holding a cyber-insurance policy decreases additional cybersecurity investment.

The first-order conditions represented by (7) and (8) are applicable when the organization's optimal additional cybersecurity investment has an interior solution. In general, the organization chooses nonzero additional cybersecurity investment if and only if (2) or (5) is nonnegative. It is possible that the organization's optimal additional cybersecurity investment is zero in the following two scenarios.

- The organization is perfectly secure thus $R(C_s, 0) = 0$ for any C_s. Optimal additional cybersecurity investment is hence zero, the origin in Fig. 1.
- The organization's expected net benefit of additional cybersecurity investment is negative for any C_s, i.e., if the concave curve in Fig. 1 falls entirely below the 45° cost line. This could be the case if the organization has little expected private loss (i.e., attack probability is small and private loss is small) and/or cybersecurity investment is ineffective at reducing the attack success rate (i.e., $R(C_s, r)$ is high).

Since $L_1 < L_0$, the latter scenario is more likely to occur with cyber-insurance.

3.6. Effects of attack probability on cybersecurity investment

Besides the organization's private loss, the optimal additional cybersecurity investment changes also with the cyber-attack threat the

attacker imposes on the organization. Fig. 2 shows how the attack probability affects the organization's choice of additional cybersecurity investment.

Similar to Fig. 1, the horizontal axis is the various levels of additional cybersecurity investment, but the vertical axis measures the expected benefits and costs of additional cybersecurity investment at different levels of cyber-attack probabilities in absence of cyber-insurance. As shown, the optimal additional cybersecurity investment increases from C_{s1}^* to C_{s2}^* when the cyber-attack probability increases from t_1 to t_2. If the organization is cyber-insured, in which case L_0 in Fig. 2 will be replaced by L_1, the organization's optimal choice of additional cybersecurity investment is still increasing in the probability of cyber attacks.

Therefore, regardless if the organization is currently insured or not, an increase in the attack probability will induce the organization to invest more in cybersecurity infrastructure.

4. A cybersecurity game between attacker and organization

In this section, we lay out the setting of a cybersecurity game between the attacker and the organization and study the best responses of the players and the game equilibrium.

4.1. Description of the game

The cybersecurity game is a two-party game between a cyber attacker and an organization. The attacker may launch cyber attacks on the organization. The attacker decides on the probability of launching an attack. Facing the cyber-attack threat, the organization first decides on whether to purchase cyber-insurance, and then decides on how much more to invest in cybersecurity infrastructure.

In the game, the organization chooses additional cybersecurity investment depending on whether the organization acquires cyber-insurance or not and hence forming the organization's cybersecurity portfolio. The attacker chooses the probability of attacking the organization. If the attack succeeds, the attacker receives a payoff of L_0 regardless of the organization's choice of cyber-insurance and cybersecurity investment; the organization loses L_0 if having no cyber-insurance and L_1 if having cyber-insurance (with the insurance company pays $(L_0 - L_1)$).

Although the insurance company pays part of the cyber incident loss when the organization is covered, the insurance company is not modeled as a player in the game to focus on the strategic interactions between the attacker and the organization. The insurance company offers pre-designed cyber-insurance products for the organization to choose from. Each cyber-insurance policy is a premium-deductible combination (hereinafter referred to as a "policy bundle") where the policy premium and the deductible are inversely related.

4.2. Organization's strategy

The organization's action space is illustrated by Fig. 3. In particular, the organization's cyber-insurance acquisition choice depends on if there exists a policy bundle that generates a net value to the organization. Of all the beneficial policies available, the organization shall choose the policy that generates the maximum net value. The detailed analysis of how the organization decides on cyber-insurance acquisition is as follows.

The cost of cyber-insurance is C_i and the expected benefit of being insured is $R(C_s^{**}, r)t(L_0 - L_1)$. The organization decides on cyber-insurance purchase to maximize expected net benefit of cyber-insurance.

$$R(C_s^{**}, r)t(L_0 - L_1(C_i)) - C_i \tag{9}$$

Recall C_i and L_1 are inversely related and C_s^{**} depends on L_1. If L_1 is continuously differentiable in C_i and the optimal cyber-insurance has

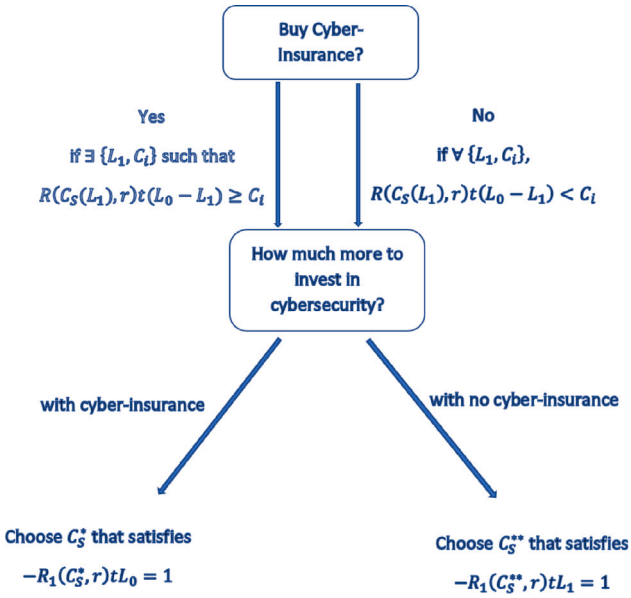


Fig. 3. The organization's action space.

an interior solution, the optimal cyber-insurance premium C_i^* solves the first-order condition of (9). If L_1 is not continuously differentiable in C_i, which is more likely to be the case, the organization would choose the optimal insurance package $\{L_1^*, C_i^*\}$ from available discrete cyber-insurance packages that generates the largest expected net benefit, i.e., $R(C_s^{**}(L_1^*), r)t(L_0 - L_1^*) - C_i^* \geq R(C_s^{**}(L_1), r)t(L_0 - L_1) - C_i$ for all $\{L_1, C_i\}$.

From (9), the organization chooses to buy cyber-insurance if it faces a high attack probability and there exists a cyber-insurance policy bundle that satisfies

$$t \geq \frac{C_i}{R(C_s^{**}, r)(L_0 - L_1)} \tag{10}$$

where the right-hand-side is the lowest attack probability making the organization willing to buy cyber-insurance, which is decreasing in L_0. It implies that compared to small- and medium-sized organizations, large organizations with high incident loss are more likely to buy cyber-insurance.

It is possible that the organization's optimal cyber-insurance does not have an interior solution. In general, the organization will not purchase cyber-insurance if the expected net benefit of cyber-insurance (9) is not positive. The organization's optimal cyber-insurance is zero in the following two scenarios.

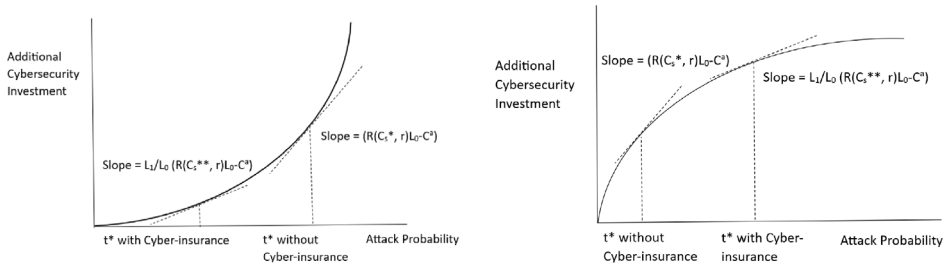
- The organization is perfectly secure thus $R(C_s^{**}(L_1), 0) = 0$ for any L_1.
- The organization's expected net benefit of cyber-insurance is negative for any $\{L_1, C_i\}$. This can be the case if the organization has little expected incident loss (i.e., attack probability is small and incident loss is small) and/or the cyber-insurance policy offered is unfavorable.

Once the organization has decided on cyber-insurance acquisition, it determines additional cybersecurity investment to complete the cybersecurity portfolio, as shown by the economic analysis in Section 3.

4.3. Attacker's strategy

The attacker launches cyber-attacks to maximize expected net payoff:

$$\max_t R(C_s(t), r)tP^a - tC^a \tag{11}$$



(a) Case I: Additional cybersecurity investment is increasing in attack probability at an increasing rate

(b) Case II: Additional cybersecurity investment is increasing in attack probability at a decreasing rate

Fig. 4. The attacker's optimal attack probability with and without cyber-insurance, depending on the organization's choice of additional cybersecurity investment in response to attacker's attack probability.

where P^a is the attacker's payoff received from a successful attack and C^a is the cost of attack. For simplicity, we assume the game between the organization and the attacker is zero sum, i.e., $L_0 = P^a$. Thus, the tri-features of the organization, (C_s, r, L_0), characterize the organization's attractiveness to the attacker. The attacker's own cost of attack, C^a, also matters. We believe that L_0 is the most important factor affecting the attacker's choice of victims. A large part of the attacker's cost is fixed initial investment such as the cost of acquiring malware, herding botnets, etc. The marginal cost of attacking an additional victim is trivial. We adopt a lump-sum cost function for the attacker. Given t, the attacker's highest possible expected net payoff is $t\{R(0,r)L_0 - C^a\} = t\{rL_0 - C^a\}$, where $rL_0 - C^a$ is the net payoff of a successful attack. This is the default benchmark of zero additional cybersecurity investment with and without cyber-insurance. As C_s increases, the attacker's expected net payoff decreases since $R(C_s, r)$ is decreasing in C_s.

Attacking the organization is profitable as long as $R(C_s(t), r)L_0 > C^a$. Whether the organization buys cyber-insurance does not affect L_0 that is either paid by the organization, the insurer, or both. $R(C_s, r)$ increases as C_s decreases.

Buying cyber-insurance is beneficial to the organization when (10) holds true. Since t is a control variable of the attacker, the attacker can affect the organization's decision to buy cyber-insurance. When t increases, the organization is more likely to buy cyber-insurance, other things constant. Nevertheless, other things are not constant. Although r and L_0 are exogenous and $\{L_1, C_i\}$ are predetermined, C_s increases with t, and hence R is decreasing in t. The attacker faces a tradeoff when raising the attack probability on the insured organization: an increase in t increases optimal additional cybersecurity investment, decreasing the attack success rate and hence the expected payoff while the increased t itself increases the expected payoff. The attacker has to control t strategically to generate a positive net gain.

With and without cyber-insurance, the attacker chooses t to solve (11). The first-order condition is

$$R'(C_s, r)\frac{dC_s}{dt}tL_0 + R(C_s, r)L_0 = C^a \tag{12}$$

Combined with (7) and (8), the attacker's optimal attack probability solves $\frac{dC_s^*}{dt} = R(C_s^*, r)L_0 - C^a$ without cyber-insurance, and $\frac{dC_s^{**}}{dt} = \frac{L_1}{L_0}(R(C_s^{**}, r)L_0 - C^a)$ with cyber-insurance.

$L_1 < L_0$, $C_s^* > C_s^{**}$ and $R(C_s^*, r) < R(C_s^{**}, r)$. The relative size of $\frac{dC_s^*}{dt}$ and $\frac{dC_s^{**}}{dt}$ depends. Facing the tradeoff, how cyber-insurance affects the attacker's optimal attack probability depends on how cybersecurity investment responds to attack probability. Suppose $(R(C_s^*, r)L_0 - R(C_s^{**}, r)L_1) > C^a(1 - \frac{L_1}{L_0})$, thus $\frac{dC_s^*}{dt} > \frac{dC_s^{**}}{dt}$. If cybersecurity investment is increasing in attack probability at an increasing rate (Fig. 4(a)), the attacker shall decrease the attack probability on the insured organization. If cybersecurity investment is increasing in attack probability at a decreasing rate (Fig. 4(b)), the attacker shall increase the attack probability on the insured organization. $\frac{dC_s}{dt}$ measures the slope of the cybersecurity investment curve. It would be the opposite if $\frac{dC_s^*}{dt} < \frac{dC_s^{**}}{dt}$.

In summary, if the attacker holds constant the attack probability, the organization's acquisition of cyber-insurance benefits the attacker by decreasing the organization's additional cybersecurity investment. The attacker may increase the attack probability to "induce" the organization to become insured. If the organization is already insured, the attacker needs to choose the optimal attack probability strategically to maximize the attack payoff. In practice, the attacker often lacks the knowledge of which organization is insured. Thus, Case II in Fig. 4 is in favor of the attacker as it justifies the consistent strategy of increasing the attack probability regardless of whether the organization is insured or not.

4.4. Game equilibrium

According to the economic analysis, the organization's purchasing cyber-insurance is beneficial to the attacker as the organization reduces additional cybersecurity investment when insured. Such potential gain for the attacker can only be realized if the organization chooses to buy cyber-insurance. The attacker may increase the cyber threat imposed on an organization to force the organization to purchase cyber-insurance. Meanwhile, if the attacker increases the attack probability on an organization that is already cyber-insured, increasing further the attack probability will make the organization invest more in cybersecurity, thus negatively affecting the benefits of the attacker. Hence, a plausible equilibrium solution is for the attacker to impose just enough cyber threat on the organization for the organization to acquire cyber-insurance. That way, the attacker plays the role of "God" to keep the organization just at the threshold of cyber insurance acquisition, thus minimizing the additional cybersecurity investment the organization chooses. The attack probability of the attacker at the threshold is

$$t^* = \frac{C_i}{R(C_s^{**}, r)(L_0 - L_1)} \tag{13}$$

At this attack probability, the organization purchases cyber-insurance and chooses an additional cybersecurity investment level of $C_s^{**}(t^*)$ (as illustrated in Fig. 1 with $t = t^*$ and private loss of L_1), and the attacker receives an expected net payoff of

$$\frac{C_i}{R(C_s^{**}(t^*), r)(L_0 - L_1)}\{R(C_s^{**}(t^*), r)L_0 - C^a\} \tag{14}$$

5. Alleviation of attacker's manipulation

In the cyber-insurance game, the attacker holds a naturally advantageous position by playing the "hand of God", but it does not mean the organization is completely passive. For example, suppose both the organization and the attacker are aware that Case II in Fig. 4 is in the attacker's favor, as counteracts, the organization shall consider the

appropriate mechanism to adjust cybersecurity investment in response to the attacker's attack probability. In this section, we discuss the implications of the game theoretic analysis with a focus on plausible countermeasures against the attacker's potential manipulation of cyber-insurance. We also relax some model assumptions to derive further insights on improving cybersecurity at the presence of cyber-insurance.

5.1. On parameters affecting organization's acquisition of cyber-insurance

Of all the variables in (10), r and L_0 are both predetermined that depend on past cybersecurity investment, i.e., they are exogenous to the organization's current decision-making. L_1 and C_i define the insurance policy bundle the organization chooses from available policy options. C_s^{**} is the organization's control variable of optimal cybersecurity investment with cyber-insurance. The range of t is between 0 and 1. If $\frac{C_i}{R(C_s^{**},r)(L_0-L_1)} > 1$, there would be no t satisfying (10), meaning the organization would not purchase cyber-insurance regardless of the attacker's choice. This may occur in the following circumstances:

1. The organization has low cybersecurity risk with existing cybersecurity investment (i.e., r is low and/or L_0 is low).
2. The cyber-insurance policy bundle is costly (i.e., C_i is high and/or L_1 is high).
3. The optimal additional cybersecurity investment is high (i.e., C_s^{**} is high) and/or the return on cybersecurity investment is high (i.e., $R(C_s^{**}, r)$ is low).

Of the circumstances, 1 is predetermined. 2 can be interpreted as common practices in the insurance industry dealing with moral hazard by increasing the shared cost of the insured. The problem of moral hazard occurs when insurance alters the insured policyholder's incentives for loss-prevention. The key to reduce moral hazard is to increase the contingent cost of cyber incident to prevent perverse incentives. Monetary costs can be recovered by cyber-insurance, but implicit costs such as damaged reputation may persist. As the share of uncovered implicit losses increases, the organization becomes less likely to purchase cyber-insurance.

We can extend the private loss of an insured organization (L_1) to include not only the deductible, but also the uncovered costs of a cyber incident including but not limited to reputation loss, uncovered monetary loss, expected increase in future premiums, etc. An increase in L_1 increases the organization's additional investment in cybersecurity, thus reducing the moral hazard problem.

5.2. Improve cybersecurity investment efficiency

Circumstance 3 in 5.1 is essential for counteracting the attacker as it is under the direct control of the organization. It implies that the organization's priority shall always be strengthening the organization efficiently. Increasing cybersecurity investment can be costly but increasing the efficiency of cybersecurity investment is the mostly cost-effective way of defending the organization against cyber attacks, regardless of the presence of cyber-insurance. When the organization decides on the allocation of limited cybersecurity investment budget, the guiding principle shall be to maximize the return on investment: to minimize $R(C_s, r)$. Return on cybersecurity investment has been commented on the importance for managing the cybersecurity defense resources (Enayaty-Ahangar et al., 2020). The modeling analysis in this research also indicates the importance of improving the efficiency of cybersecurity investment for reducing the attacker's potential manipulation of cyber-insurance.

The "no cyber-insurance" or "little cyber-insurance" strategy is a dominant strategy in the extreme cases of the three circumstances in 5.1 because in these circumstances buying cyber-insurance does not general net benefits regardless. The derived general principle of reducing the leeway of the attacker's manipulation of cyber-insurance is to decrease the net marginal return on t, either via increasing the marginal cost or decreasing the marginal benefit of the increased t.

From (11), the attacker's net marginal return on t is $RP^a + R'tP^a - C^a$ where $R' < 0$. Holding the cost of launching attacks constant, the attacker's return on attack depends on the tradeoff between RP^a and $R'tP^a$. Borrowing the term of price elasticity of supply or demand, we define the attack elasticity of cybersecurity investment (denoted as $\epsilon_a = -R't/R$). Approximately, the attacker's expected revenue and the attack elasticity of cybersecurity investment have the following relationship.

1. If $\epsilon_a > 1$, $R(C_s(t), r)tP^a$ decreases when t increases.
2. If $\epsilon_a = 1$, $R(C_s(t), r)tP^a$ is unchanged when t changes.
3. If $\epsilon_a < 1$, $R(C_s(t), r)tP^a$ increases when t increases.

Hence the attacker shall decrease the attack probability to increase revenue in the first scenario and increase the attack probability to increase revenue in the third scenario. The first scenario is the case that the attacker is less likely to manipulate cyber-insurance because the attacker's potential of inducing the organization to purchase cyber-insurance lies in the attacker's ability to raise the attack probability to or above the threshold. Realizing the first scenario requires increased effectiveness of cyber defense as cybersecurity investment increases at a higher t. That is, when R decreases at increased C_s due to a higher t, the decrease in R exceeds the increase in t, resulting in a net decrease in the attacker's payoffs.

Unfortunately investment is often subject to diminishing returns. Compared to business fixed investment, cybersecurity investment has the advantage of diversification. As the organization becomes increasingly networked and distributed, strengthening cybersecurity involves enhancing hardware, software, networks, data, people, and integration with the physical world. Although continuous investment defending against a certain type of cyber attacks may be subject to diminishing returns, the organization can select among various cyber attacks as well as different defense tools to maximize the marginal return on additional cybersecurity investment.

5.3. Link cyber-insurance premium to cybersecurity investment

In the model, we assume the premium on cyber-insurance depends on existing cybersecurity investment but not additional investment the organization will choose after being insured. That is, we consider the situation that current cyber-insurance premium is linked to the organization's cyber history, gauged by the organization's previous cybersecurity investment choice and the record of cyber incidents. It is possible that the insurance company forecasts the impact the purchase of cyber-insurance may have on cybersecurity investment and links premium to the organization's additional cybersecurity investment. In other words, cyber-insurance premium still changes with the breadth of coverage and the deductible, which sets a base rate, but the actual premium paid by the organization fluctuates with its choice of additional cybersecurity investment. In this case, the optimal additional cybersecurity investment solves

$$\max_{C_s}[r - R(C_s, r)]tL_1 - C_s - C_i(C_s) \tag{15}$$

The organization's optimal additional cybersecurity investment, C_s^{**} can be derived from the first-order-condition of (15)

$$-R'(C_s^{**}, r) = \frac{1}{tL_1}(1 + \frac{dC_i}{dC_s}) \tag{16}$$

where $R_1(C_s^{**}, r) < 0$ and $-R_1(C_s^{**}, r)tL_1$ measures the slope of the lower curve in Fig. 1. Optimal additional cybersecurity investment increases when the slope decreases. Compared to (8), since $\frac{dC_i}{dC_s} < 0$ and $(1 + \frac{dC_i}{dC_s}) < 1$, the organization's choice of additional cybersecurity investment with cyber-insurance increases if the current

policy premium depends on both the existing status of cybersecurity investment and also the additional cybersecurity investment. In practice, cyber-insurance issuers shall make the assumption that the purchase of cyber-insurance can have some impact on investment into the cybersecurity and hence price it in.

Therefore when cyber-insurance premium is inversely linked to additional cybersecurity investment, optimal additional cybersecurity investment increases. In principle, the insurer can create a cybersecurity investment incentive mechanism to bring the organization's optimal additional cybersecurity investment close to the insurance-absent level. If it can even go above it, the attacker will be worse off at the presence of cyber-insurance. In practice, the market for cyber-insurance does not have the refined premium setting standards that exist with more established lines of insurance. While the financially-driven organization builds the optimal cybersecurity portfolio, the insurer shall work on building a pricing model that counteracts the disincentives cyber-insurance may impose on cybersecurity investment. Further research is needed to extend to cyber-insurance pricing models with finer adjustments in premium, deductible and organization-specific factors such as the cybersecurity records of the organization.

5.4. Play a game of secrecy

Another plausible defense measure is with information. An implicit assumption of the model is complete information: the attacker knows if the organization is currently insured and has access to the information for estimating the threshold of attack probability to induce the organization to buy cyber-insurance; the organization knows the confronted cyber threat (i.e., the likelihood of being attacked). In practice however, neither is guaranteed. The attacker is uncertain whether the target organization is currently insured, due to, for example, lack of past records of the organization's changed coverage status. On the other hand, it is hard for the organization to estimate the pending cyber risk, also due to lack of information.

It is widely recognized that private information has value and the more informed party playing a game with hidden information and even deception benefits from it. As countermeasures, it is necessary for the organization to keep the acquisition of cyber-insurance private information unreleased to the attacker. Other important hidden information is the cyber incident loss and the cyber vulnerability of the organization. The organization shall keep the choice of cybersecurity investment and cyber-insurance hidden information unknown to the cyber attacker. That way, the attacker's choice of targets would have to base on publicly known factors such as the size of the organization (Kamiya et al., 2018). Keeping the key information hidden to the attacker and/or somehow signaling fake information to mislead the attacker will restrict the attacker's plausible manipulation of cyber-insurance.

Furthermore, the organization benefits not only from keeping its own information private, but also from hidden information of other organizations. After all, relevant information to the attacker includes not merely the information on the organization itself, but also on similar organizations and related organizations such as competitors, suppliers and clients. Some organizations are content with their own cybersecurity protections. Some do not want to pay the premium. If all organizations keep private information of their cyber-insurance choices hidden to the attacker, they form a mutual "social defense network". In this network, heterogeneous organizations with various vulnerability, cybersecurity investment and cyber-insurance coverage provide "social insurance" for each other at zero additional financial costs, an analogy to optimal social insurance discussed in Liao et al. (2012).

5.5. Role of government

Further extension of the analysis is to consider possible government actions on cyber-insurance. Governments can certainly play a role as the market regulator. Mature insurance markets collectively pool and distribute risks but private governance struggles when markets grow too big for informal coordination or when risks escalate, the so-called "market failure" as related to adverse selection and moral hazard. Governments can support insurance markets to maintain insurability and limit risks to society. Government interventions vary widely. A conceptual framework is proposed to group government interventions into three dimensions: regulation of risky activity, public investment in risk reduction, and co-insurance (Baker and Shortland, 2022). The priority can be supporting economic activity, risk reduction or ex post socialization of losses.

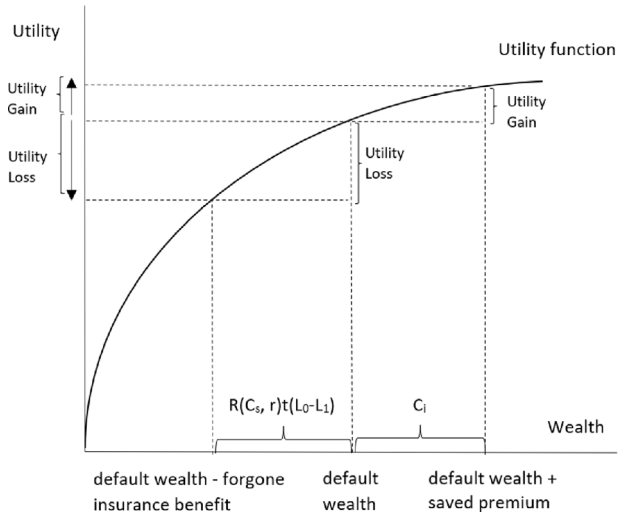


Fig. 5. Risk-averse organization's utility function.

With government intervention, two extreme cases can wipe out the attacker's ability of manipulating cyber-insurance by changing attack probability: banning cyber-insurance when no organizations can buy cyber-insurance or mandatory cyber-insurance when all organizations are required to buy cyber-insurance. This is the job of government regulation. Insurance regulation is meant to reduce moral hazard and adverse selection prevailing insurance markets rather than killing the markets. The prohibition of cyber-insurance options is highly unlikely to be adopted by the government. Compulsory cyber-insurance nevertheless, is plausible. Compulsory insurance is any type of insurance that legally requires an individual or organization to purchase. There exist compulsory auto insurance and health insurance. In practice, it is often not in insurers' or the organizations' interests to engage in the kinds of loss prevention efforts that security experts recommend and governments more frequently mandate or undertake themselves (Abraham and Schwarcz, 2022).

Governments can decide on what type of insurance is mandatory and how much coverage policyholders have to buy. Policyholders normally are free to purchase higher limits of coverage beyond the legal minimum. Compared to auto insurance or health insurance, cyber-insurance can be more sophisticated. The types of cyber incidents and losses are broad and complex. It is impossible for the government to mandate the purchase of cyber-insurance to cover everything. The welfare and security effects of government regulation are uncertain. For organizations whose optimal cybersecurity investment on infrastructure and/or cyber-insurance is within the legal minimum anyway, government regulations will have no real effects.

5.6. When organization is risk averse

In the modeling analysis, the organization is assumed to be risk neutral. To the risk-neutral organization, the financial investment in cybersecurity breaks even when the sure spending on cybersecurity

is equal to the mathematical expected benefits the investment will generate. Therefore the benefits and the costs of an equal amount are valued equally by the organization, certain or expected. In practice, an organization can be risk-averse rather than being risk-neutral. When the organization experiences a loss in market value when an attack happens and this loss is not covered by cyber-insurance, the organization may value the loss more than an equal amount of benefit.

To capture the risk-aversion intuition, the common approach in economics is to use the model of expected utility in which risk aversion derives from diminishing marginal utility for wealth. Fig. 5 illustrates how utility for wealth changes with cyber-insurance for a risk-averse organization. Wealth can be interpreted as monetary assets of the organization. Given an arbitrary level of wealth (labeled as "default wealth" in Fig. 5), if the organization does not purchase cyber-insurance, the organization does not have to pay the premium of C_i. The utility associated with the saved premium is indicated as "utility gain" in the figure, but not having cyber-insurance coverage has an opportunity cost of forgone possible insurance benefit of $R(C_s, r)t(L_0 - L_1)$. The utility associated with the opportunity cost is indicated as "utility loss" in Fig. 5. At the risk-neutral cyber-insurance break-even point $R(C_s, r)t(L_0 - L_1) = C_i$, a risk-neutral organization (with a linear utility function not drawn in Fig. 5) is indifferent between being covered or not but a risk-averse organization (with a concave utility function drawn in Fig. 5) will choose to buy cyber-insurance as the expected utility loss of not being insured exceeds the utility gain. Therefore, a risk-averse organization is more likely to purchase cyber-insurance than a risk-neutral organization in similar financial circumstances and can accept a higher premium on similar cyber-insurance policy bundle. The break-even cyber-insurance premium can be found graphically in Fig. 5 at which "Utility Gain = Utility Loss", given the policy benefits specified by $R(C_s, r)t(L_0 - L_1)$. Apparently, such break-even premium is higher than C_i.

From above, a risk-averse organization values a loss more than a gain of an equal amount. The net benefit function (9) that works for a risk-neutral organization needs to be rewritten as the following for a risk-averse organization where the utility function $U(\cdot)$ is diminishing.

$$U(R(C_s, r)t(L_0 - L_1(C_i))) - U(C_i) \tag{17}$$

The cyber-insurance break-even point for a risk-neutral organization occurs at $R(C_s, r)t(L_0 - L_1) = C_i$ while the cyber-insurance break-even point for a risk-averse organization occurs at $R(C_s, r)t(L_0 - L_1) < C_i$. To receive the same expected net benefit from cyber-insurance, $R(C_s, r)$ must be smaller in the risk-averse case than the risk-neutral case, therefore the optimal additional cybersecurity investment with cyber-insurance (C_s^{**}) is bigger in the risk-averse case than the risk-neutral case. Note the risk-averse organization's optimal additional cybersecurity investment will also increase with no cyber-insurance.

To summarize, if the organization is risk averse rather than risk neutral, the organization has more incentives to buy cyber-insurance and make more additional investment in cybersecurity infrastructure with and without cyber insurance. The former may be beneficial to the attacker but not the latter. Compared to the risk-neutral case, the attacker has stronger incentives to impose the "just right" amount of cyber-attack threat to push the risk-averse organization to reach the threshold of acquiring cyber-insurance so that the organization shifts from not buying cyber-insurance to buying cyber-insurance, consistent with and even strengthening the key findings of this research.

6. Simulation and case study

In this section, we conduct a more practice oriented numerical analysis of a hypothetical company, a national retailer, on its cyber-insurance acquisition and cybersecurity investment decisions. We especially analyze the attacker's strategy and its impacts on the company's strategy, based on assigned values of parameters rather than actual data gathered from a certain company. The high-level abstraction is used to allow for identification of general insights applicable to a broad range of situations.

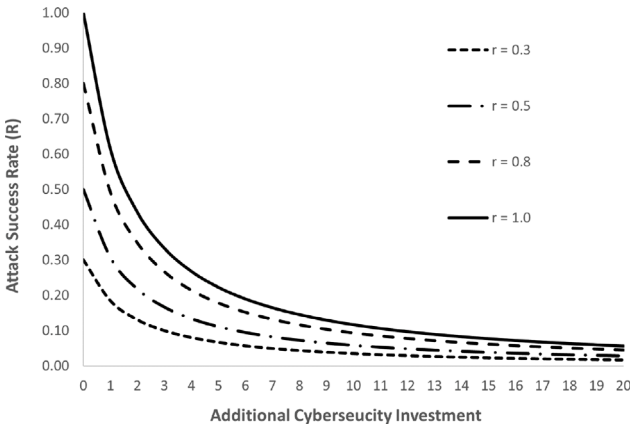


Fig. 6. Organization benefits from additional cybersecurity investment with decreasing attack success rate at a diminishing effect.

The retailer's risk manager, Amy, is responsible for managing the budget and operation of cybersecurity investment. As the company begins to scale, particularly digitally, cybersecurity risk increases. Amy is aware of cyber-insurance and knows it is time to reevaluate the company's cyber risk and the formation of a cybersecurity portfolio composed of both cybersecurity investment and cyber-insurance to address the possibility of cyber attacks.

Amy faces the problem of how much more the company should invest in cybersecurity, given a breach probability function of $R(C_s, r)$ linking the cyber vulnerability of the company inversely to the additional resources the company devotes to cybersecurity investment. She uses the following functional form to quantify the inverse relationship in her numerical analysis. The function depends on two factors, the existing vulnerability of the company and how much more the company is investing in cybersecurity.

$$R(C_s, r) = \frac{r}{(\alpha C_s + 1)^{\beta}} \tag{18}$$

where $\alpha > 0$ and $\beta \geq 1$ are parameters that govern the efficiency of the investment. $R(C_s, r)$ is decreasing in both α and β. Such a R function has a relatively simple functional form and satisfies all the three features the function shall have, as specified in 3.1. Relatively standard parametrization are chosen as $\alpha = 0.5$ and $\beta = 1.2$ without loss of generality as the insights derived from the numerical results will hold true for all values of $\alpha > 0$ and $\beta \geq 1$. The numerical analysis can be repeated readily with different values of the parameters as the company sees fit.

6.1. Cyber vulnerability, cybersecurity investment and cyber-insurance

Using the attack success rate at existing cybersecurity investment as a measure of the cyber vulnerability of the company, Amy analyzes scenarios with different cyber vulnerability to have an overview of the effectiveness of additional cybersecurity investment on improving the cyber strength of the company. In particular, she considers $r = 0.3$, $r = 0.5$, $r = 0.8$, and $r = 1.0$. A higher r indicates higher cyber vulnerability. $r = 1$ is extreme cyber vulnerability, meaning the company would fall victim once chosen as a target by the attacker. $R(C_s, r)$ decreases when C_s increases. The reduced attack success rate with additional cybersecurity investment is calculated using (18).

Fig. 6 shows how the attack success rate changes with additional cybersecurity investment at various levels of existing cyber vulnerability. As shown, while the attack success rate decreases with cybersecurity investment, cybersecurity investment cannot reduce the attack success rate to zero. Unless the company is perfectly secure that does

not require additional cybersecurity investment (i.e., $r = 0$), the company, which is vulnerable to cyber-threat, will benefit from cybersecurity investment. However, the company cannot be 100% secure with additional cybersecurity investment.

The results imply that increasing cybersecurity investment infinitely is not optimal (and not viable, either). Marginal cost–benefit analysis is required to determine the optimal amount of cybersecurity investment without and with cyber-insurance. The marginal effect of cybersecurity investment can be found by solving for the partial derivative of (18) with respect to C_s,

$$R'(C_s, r) = -\beta\alpha r(\alpha C_s + 1)^{-1-\beta} \tag{19}$$

Combining (7) and (8) with (19), the optimal additional cybersecurity investment without and with cyber-insurance is the following:

$$C_s^* = \frac{(\alpha\beta r t L_0)^{\frac{1}{1+\beta}} - 1}{\alpha} \tag{20}$$

$$C_s^{**} = \frac{(\alpha\beta r t L_1)^{\frac{1}{1+\beta}} - 1}{\alpha} \tag{21}$$

Based on recent retail cybersecurity statistics, Amy estimates that the company faces a cyber-attack threat of 30% (i.e., $t = 0.3$) and a cyber incident loss of $100 million (i.e., $L_0 = 100$). Suppose the available cyber-insurance plans offer three options of deductibles, $L_1 = 80$, $L_1 = 50$, and $L_1 = 20$, referred to as the high-, medium-, and low-deductible insurance policy. Amy calculates optimal cybersecurity investment without insurance and with insurance of different deductibles at various cyber vulnerability. Fig. 7 shows the results. The horizontal axis measures the attack success rate at existing cybersecurity investment. The vertical axis is the company's optimal additional cybersecurity investment. The intersection of any curve and the horizontal axis is the *critical point* or *threshold* of the attack success rate at existing cybersecurity investment: beyond which the company should invest more in cybersecurity and choose C_s^* or C_s^{**} as plotted; below which $C_s = 0$.

Amy finds that the company should not invest more in cybersecurity with low cyber vulnerability. From (20) and (21), optimal additional cybersecurity investment equals zero until $r = \frac{1}{\alpha\beta t L_0}$ without cyber-insurance and $r = \frac{1}{\alpha\beta t L_1}$ with cyber-insurance. At the specified parameters, the former is 5.6% and the latter is 7%, 11% and 28%, at $L_1 = 80$, $L_1 = 50$, and $L_1 = 20$, respectively. As private loss decreases, the company's optimal cybersecurity investment decreases.

Key observations of Fig. 7 include: (1) As the attack success rate increases, optimal additional cybersecurity investment increases, insured or not; (2) Being insured decreases optimal additional cybersecurity investment. The decrease is increasing in the coverage of cyber-insurance; (3) Being insured increases the critical point (threshold) of additional cybersecurity investment. The threshold is increasing in the coverage of cyber-insurance.

Concerned with the high uncertainty in the probability of being attacked, Amy decides to calculate the company's optimal cybersecurity investment at various attack probabilities. She assesses the existing cybersecurity investment of the company and estimates that the company's current cyber-vulnerability is $r = 50\%$. Fig. 8 shows how optimal additional cybersecurity investment is affected by the attacker's changing attack probability. Similar to Fig. 7, insurance policies of various coverage are compared with each other and the no-insurance case.

As expected, Amy finds that the company's optimal additional cybersecurity investment shall increase with increased attack probability. The intersection of any curve and the horizontal axis is the *critical point* or *threshold* of attack probability for the company to start investing more in cybersecurity. The company shall choose no additional cybersecurity investment ($C_s = 0$) if the attack probability is below the critical point. From (20) and (21), optimal additional cybersecurity investment equals zero until the attack probability reaches $t = \frac{1}{\alpha\beta r L_0}$ without cyber-insurance and $t = \frac{1}{\alpha\beta r L_1}$ with cyber-insurance. At the specified parameters, the former is 3.3% and the latter is 4.2%, 6.7% and 16.7%, at $L_1 = 80$, $L_1 = 50$, and $L_1 = 20$, respectively. Purchasing cyber-insurance decreases cybersecurity investment and a low-deductible cyber-insurance coverage reduces much cybersecurity investment. The findings suggest that the attacker's attack probability can affect the company's choice of optimal additional cybersecurity investment.

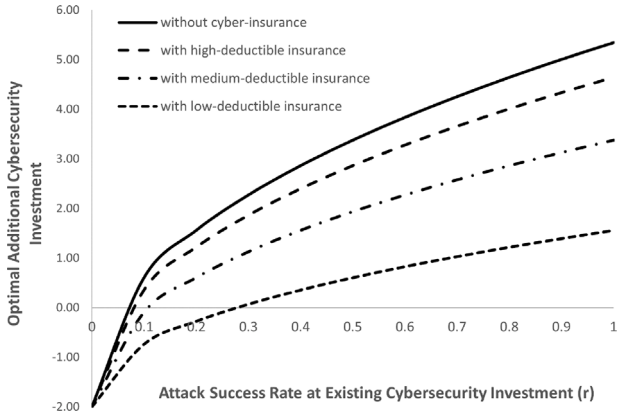


Fig. 7. While optimal additional cybersecurity investment (insured or not) increases when attack success rate at existing cybersecurity investment rises, cyber-insurance actually reduces optimal cybersecurity investment and increases the critical point (threshold) of cybersecurity investment. Organizations will not invest in additional cybersecurity below the critical point.

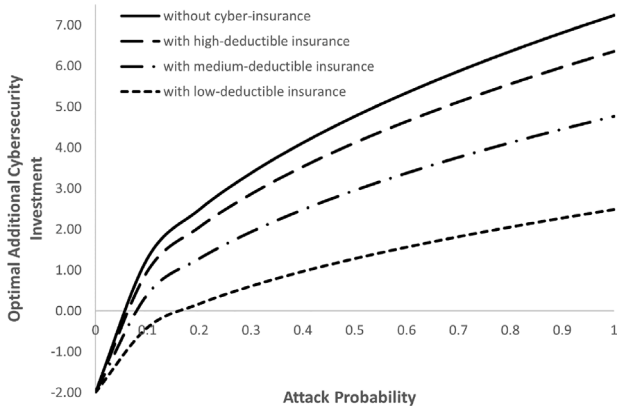


Fig. 8. While optimal additional cybersecurity investment (insured or not) increases when attack probability rises, cyber-insurance actually reduces optimal cybersecurity investment and increases the critical point (threshold) of cybersecurity investment. Organizations will not invest in additional cybersecurity below the critical point.

Amy notices that r and t play similar roles in affecting cybersecurity investment. The similarity of Figs. 7 and 8 reflects the symmetry of r and t in (20) and (21). After all, the two parameters combined (i.e., $t \times r$ measuring the attacker's likelihood of launching a successful attack) determines the overall cyber risk the company faces.

Amy also estimates optimal additional cybersecurity investment as a percentage of the expected cyber-attack loss ($t \times r \times L_0$) without and with cyber-insurance of different deductibles. Fig. 9 shows the estimates. Although the dollar amount of cybersecurity investment increases with rising expected loss, additional cybersecurity investment as a percentage of expected loss is not consistently increasing. In most cases, there is a noticeable jump in the percentage when the company starts investing more in cybersecurity facing larger expected loss, but the percentage then gradually falls. If the company acquires cyber-insurance with low deductible, additional cybersecurity investment compared to expected loss rises gradually but overall the optimal amount of cybersecurity investment is only a small fraction of the expected loss.

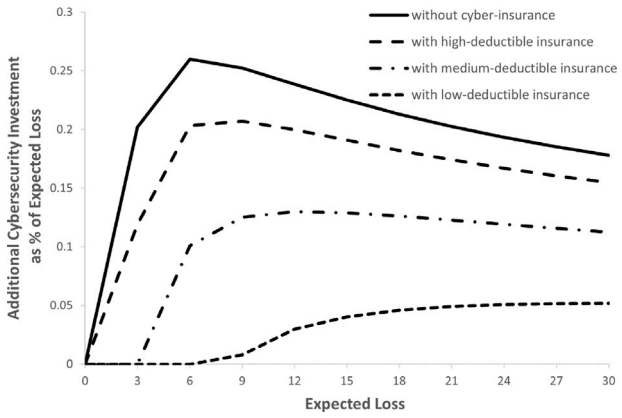


Fig. 9. Generally, optimal additional cybersecurity investment as a percentage of the expected cyber incident loss first rises and then falls as the expected loss increases. For cyber-insurance policies with low deductibles, optimal additional cybersecurity investment as a percentage of the expected loss gradually increases and overall, remains as a small fraction of the expected loss.

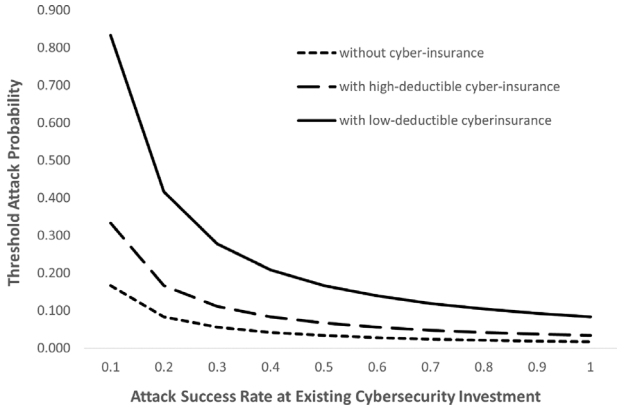


Fig. 10. Cyber-insurance raises the critical point (threshold) of attack probability thus decreases the organization's likelihood to increase cybersecurity investment. The attacker may influence the organization's choice of additional cybersecurity investment by choosing attacks strategically.

6.2. Effects of attacker's strategy on cybersecurity investment and cyber-insurance

Amy would like to know better about the impacts of the attacker's actions on the company's choice of additional cybersecurity investment and cyber-insurance.

Amy first studies the effects of the attacker's attack strategy on the company's cybersecurity investment decision-making. Fig. 10 shows the critical point or the threshold of attack probability that would initiate additional cybersecurity investment with and without cyber-insurance at various attack success rate. The results suggest that the attacker can influence the company's choice of cybersecurity investment by choosing attack probability strategically. For example, if cyber-insurance reduces the company's private loss of cyber incident to equaling 20% of the total incident loss and if the attack success rate at existing cybersecurity investment is 40%, an attack probability of 20.8% would trigger the company to invest more in cybersecurity.

Amy then studies the effects of the attacker's strategy on the company's choice of cyber-insurance. Given the company's cash flows and risk preference, she wants to compare cyber-insurance bundles with a high or a low deductible. She contacts the company's insurance provider for quotes on premiums for policies with different deductibles. Unlike regulatory compliance, there is no "one-size-fits-all" security framework required by insurance companies. The company's insurance

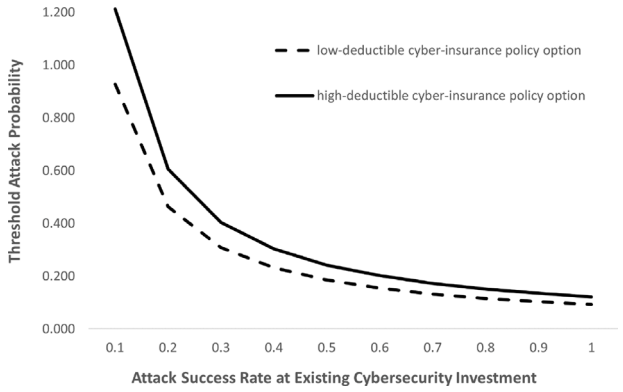


Fig. 11. If the attack probability is below the critical point (threshold), the organization will not buy cyber-insurance. The attacker may strategically choose an attack probability that will trigger the organization to buy cyber-insurance that benefits the attacker.

provider largely uses the triple probabilities as proxies quantifying the threat landscape of the company, i.e., $\{t, r, R(C_s, r)\}$ along with the cyber incident loss, L_0, are used to estimate the financial risk of insuring the company. Amy fills in the answers to a list of dozens of questions related to security controls and strategies. By assessing the cyber threats in the retail industry and the existing cybersecurity investment of the company, the insurance provider agrees upon Amy's estimates of the company's cyber attack probability of 30% and the cyber incident loss of $100 million, and provides Amy with two quotes on a "high deductible + low premium" bundle and a "low deductible + high premium" bundle: Policy A specified as $\{L_1 = 50, C_i = 3\}$; Policy B specified as $\{L_1 = 20, C_i = 7\}$, all in millions.

The company would choose to purchase a policy bundle $\{L_1, C_i\}$ if

$$R(C_s^{**}, r)t(L_0 - L_1) \geq C_i \tag{22}$$

From (18),

$$R(C_s^{**}, r) = \frac{r}{(\alpha C_s^{**} + 1)^{\beta}} \tag{23}$$

Combined with (21),

$$R(C_s^{**}, r) = \frac{r}{(\alpha\beta r t L_1)^{\frac{\beta}{1+\beta}}} \tag{24}$$

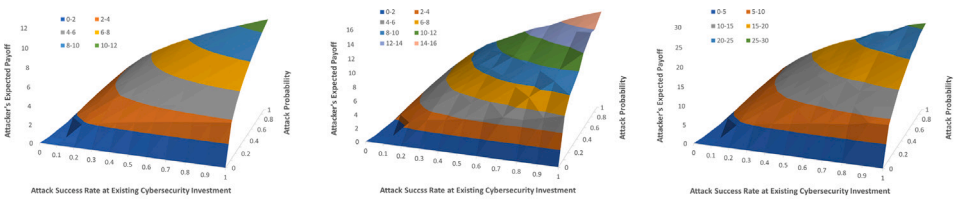
Combined with (22), Amy finds that the policy bundle $\{L_1, C_i\}$ is beneficial when facing an attack probability

$$t \geq \{\frac{C_i(\alpha\beta r L_1)^{\frac{\beta}{1+\beta}}}{r(L_0 - L_1)}\}^{1+\beta} \tag{25}$$

where the right-hand-side is the critical point or the threshold that the attacker can choose to trigger the company to buy cyber-insurance.

Amy learns from (25) the insights on the role of parameters' configuration on the company's choice of cyber-insurance and the attacker's best response. The condition would fail when the right-hand term is larger than one that could occur at $C_i(\alpha\beta r L_1)^{\frac{\beta}{1+\beta}} > r(L_0 - L_1)$, in which case, the company would not choose cyber-insurance regardless of the attacker's strategy. The cyber-insurance-policy specification $\{L_1, C_i\}$ is among the key variables determining the value of the right-hand term. In a way, the attacker and the insurer may have aligned interests to induce the company to choose cyber-insurance, hence the efforts of insurance companies to promote cyber-insurance can serve the purpose of cyber attackers.

Amy calculates the threshold of attack probability at various attack success rates and various available cyber-insurance policy bundles as in Fig. 11. The company does not buy cyber-insurance if the attack probability is below the threshold. The threshold attack probability decreases if the company is more vulnerable to cyber attacks (higher attack success rate). In the case the calculated threshold attack probability



(a) Without Cyber-Insurance (b) With High-deductible Cyber-insurance (c) With Low-Deductible Cyber-insurance

Fig. 12. The attacker's expected payoff grows from having no cyber-insurance (a) to having cyber-insurance (b and c).

is above 1.0, the company does not buy cyber-insurance regardless. At Amy's assessed exiting vulnerability of 50%, it is beneficial for the company to acquire cyber-insurance when the attack probability on the company reaches 18.5% if the company prefers a low-deductible policy and 24.2% if the company prefers a high-deductible policy.

To what degree are cybersecurity investment and cyber-insurance substitutes? Amy compares the threshold attack probability that would trigger the company to invest more in cybersecurity when the company is cyber-insured or not. The results show a significant increase in the threshold attack probability if the company is cyber-insured. At the estimated cyber vulnerability of 50% ($r = 0.5$), an attack probability of 3.3% would trigger the company to invest more in cybersecurity without cyber-insurance but the threshold attack probability increases to 6.7% if the company holds a high-deductible policy and 16.7% if the company holds a low-deductible policy. Approximately, holding a high-deductible policy reduces the company's incentives to invest in cybersecurity by about a half; holding a low-deductible policy reduces her company's incentives to invest in cybersecurity by about three-fourth.

6.3. Attacker's expected payoff and attack strategy

Realizing the company's decision-making hinges on the attacker's actions, Amy decides to do a role play and acts out the attacker. Combining (11), (18) and (20) and ignoring C^a, the attacker's expected benefit is

$$\frac{r}{(\alpha\beta r t L_0)^{\frac{\beta}{1+\beta}}} t L_0 \tag{26}$$

where L_0 in the denominator is replaced by L_1 in case of cyber-insurance.

Fig. 12 compares the attacker's expected payoff in three scenarios: without cyber-insurance, with high-deductible cyber-insurance and with low-deductible cyber-insurance. The attacker's cost function is largely composed of fixed or sunk cost in acquiring knowledge and malware to launch attacks. The marginal cost (i.e., additional cost occurred on attacking one more target) is trivial. Moreover, the fixed cost is the same with and without cyber-insurance. It is canceled out for comparison purpose. As shown in Fig. 12, the peak payoff increases from range 10–12 12(a) to range 14–16 12(b), then to range 25–30 12(c), all in millions. Amy learns that as the company's optimal cybersecurity investment is decreasing in cyber-insurance coverage, her analysis shows that the attacker benefits from the company's purchasing cyber-insurance and benefits further if the company chooses low-deductible policy bundles.

Experiences tell Amy that almost all retail cyber attacks have financial motives. The attacker does not care who shoulders the cyber incident loss, the company or the insurer. The attacker cares about the company's chosen additional cybersecurity investment. For both the attacker and the company nevertheless, cyber-insurance matters because the company's optimal cybersecurity investment depends on if the company is cyber-insured, which affects the attacker's expected payoff that the attacker can in turn affect through the attack probability. How does the attacker's strategy of attack probability affect the attacker's attack success rate and expected payoff?

Fig. 13(a) shows how the attack success rate with additional cybersecurity investment (the R function) changes with attack probability under cyber-insurance Policy A and Policy B. Amy finds that the relationship between the attacker's attack probability and the attack success rate is not unidirectional. The attacker faces a tradeoff between R and t. The curves in Fig. 13(a) are initially downward-sloping because as the attacker increases attack probability, the company increases cybersecurity investment, thus decreasing the attack success rate. There is a noticeable jump when the attack probability reaches the critical threshold that triggers the company to buy cyber-insurance. Beyond the threshold the R function gradually decreases as the company increases cybersecurity investment with rising cyber risk.

Fig. 13(b) shows how the attacker's expected payoff changes with attack probability. Similar to 13(a), there is a noticeable jump at the critical threshold. Amy understands although the analysis shows a continuous increase in the attacker's expected payoff in the figure, the net change in the attacker's expected payoff beyond the threshold is ambiguous. Many factors affecting the ambiguity (such as the pricing of cyber-insurance policy, the amount of incident loss, the attacker's increased cost as the attack probability increases, etc.) are simplified or ignored in her calculation. What is certain is the attacker's significant increase in expected payoff when setting the attack probability around the threshold to induce the company to purchase cyber-insurance, regardless if the company chooses a low-deductible or a high-deductible policy bundle. The attacker benefits the most if the company chooses a low deductible policy.

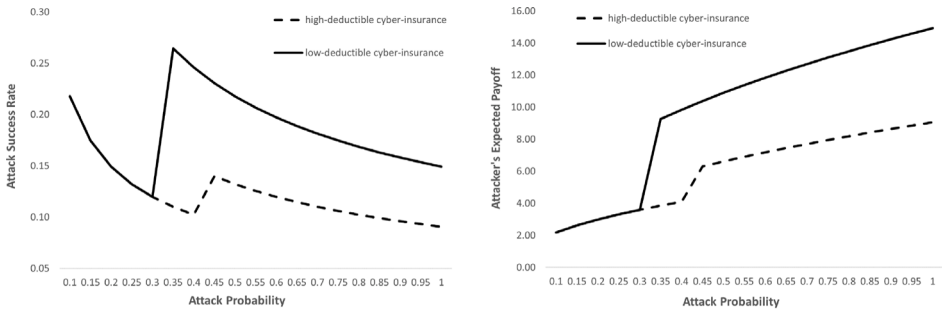
Suppose the attacker sets the attack probability initially at 20%. Under the low-deductible cyber-insurance Policy B for example, the company with cyber risk of 30% does not buy cyber-insurance, invest $C_s^* = 1.56$, and $R(1.56, 0.3) = 0.15$. The attacker's corresponding expected payoff is $0.15 * 0.2 * 100 = 3$. If the attacker increases the attack probability to 40% thus the company buys cyber-insurance, the company invests $C_s^{**} = 0.36$ and $R(0.36, 0.3) = 0.25$. The attacker's corresponding expected payoff increases to $0.25 * 0.4 * 100 = 10$.

Empowered with the possible manipulation of the critical point, the attacker may strategically adjust the attack probability to trigger the company to buy cyber-insurance thus significantly increasing expected payoffs.

6.4. Cybersecurity portfolio

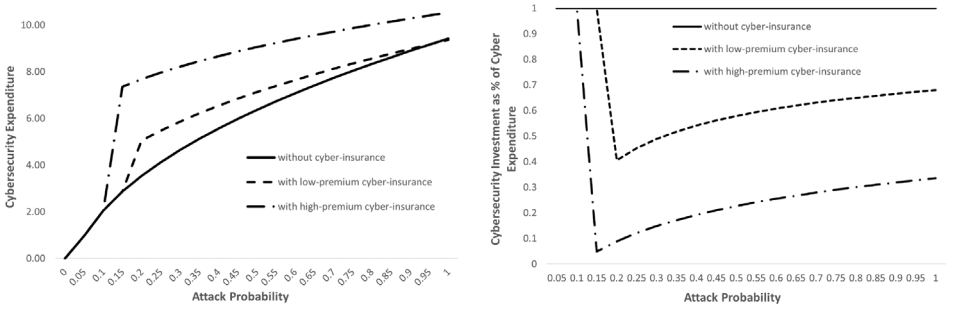
Amy now shifts from security to finance to study how the size and the composition of the company's cybersecurity portfolio can be affected by the attacker's actions. In particular, the cybersecurity portfolio includes both cybersecurity investment and cyber-insurance. Without cyber-insurance, the company's total expenditure on cybersecurity investment is C_s^*. When the company is covered by cyber-insurance, its total expenditure on cybersecurity portfolio is $C_s^{**} + C_i^*$.

Fig. 14(a) shows how the company's total cybersecurity expenditure changes with attack probability. Total cybersecurity expenditure increases regardless, indicating an increased spending on cybersecurity when the company faces increased attack probability. Given the parameters used in the numerical analysis, especially the significant



(a) Critical point affects attack success rate (b) Critical point affects attacker's payoff

Fig. 13. How are the attack success rate and attacker's expected payoff affected by the attack probability (controlled by attacker) under various cyber-insurance policies? There is a noticeable increase in the attack success rate and the attacker's expected payoff at the critical point where the organization shifts from no cyber-insurance to purchasing cyber-insurance.



(a) Total cybersecurity expenditure rises sharply at the critical point (b) Share of cybersecurity investment drops sharply at the critical point

Fig. 14. Attacker's manipulating attack probability may significantly increase organization's total cybersecurity expenditure through purchasing cyber-insurance at the critical point. The share of cybersecurity investment decreases significantly at the critical point of attack probability due to purchasing cyber-insurance and bounces back gradually after being insured.

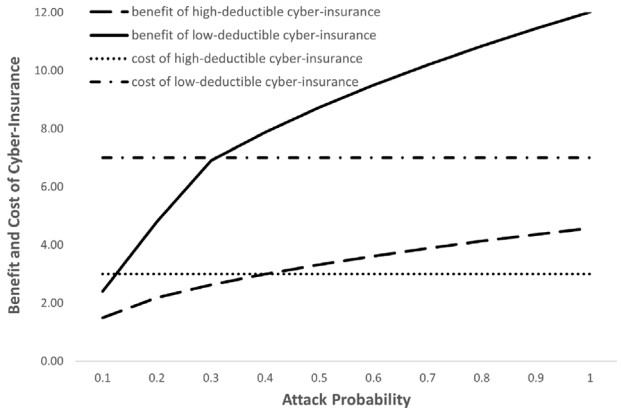


Fig. 15. Organization chooses a cyber-insurance policy with higher expected net value (expected benefit minus cost), in this case, the low-deductible policy.

premium compared to optimal additional cybersecurity investment, total cybersecurity expenditure increases sharply at the critical point.

Fig. 14(b) is cybersecurity investment as a fraction of the total expenditure. The share of cybersecurity investment falls sharply at the critical point when the company buys cyber-insurance and the share bounces back as the company increases cybersecurity investment at increasing attack probability.

Amy refers to $C_s^{**} + C_i^*$ as the "optimal cybersecurity budget" that she would propose to the company. She believes the company should not set a fixed budget on the cybersecurity portfolio. Had the company had a fixed budget nonetheless, the objective would be to achieve marginal utility equalization between cybersecurity investment and cyber-insurance. Consider a model of the company contemplating to achieve the highest possible loss evasion at a fixed cybersecurity budget B. The fixed budget is allocated to additional cybersecurity investment (C_s) and cyber-insurance (C_i). The allocation of the budget can be solved as

$$\begin{aligned} &\max_{C_s} = [r - R(C_s, r)]tL_1 - C_s - C_i \\ &\text{s.t.} C_s + C_i \le B \end{aligned} \tag{27}$$

The optimal additional cybersecurity investment derived from the first-order-condition of (27) solves

$$-R'(C_s^{**}, r) = \frac{1+\lambda}{tL_1} \tag{28}$$

where λ is the Lagrangian coefficient.

Comparing (28) and (8), since R' is increasing in C_s and $\lambda > 0$, in case of a fixed budget rather than the optimal budget, the company's optimal additional cybersecurity investment decreases further with cyber-insurance. From the cybersecurity perspective, it is preferred that the company manages the optimal budget instead of a fixed budget.

6.5. Choose cyber-insurance policy

Amy's analysis so far has been considering all available cyber-insurance bundles. Which insurance bundle should the company eventually choose? Assuming the company is risk neutral, the preferred policy is the policy that has the highest expected net value. Amy compares the net expected benefit (expected benefit minus cost) of the high-deductible and low-deductible policy bundles.

Amy plots the company's expected benefit and cost of purchasing either the high-deductible Policy A or the low-deductible Policy B in Fig. 15. The straight lines show the costs (the premium) of the policy bundles and the curves show the benefits. The vertical distance between

the benefit curve and the cost line is the expected net benefit of a particular policy bundle. As shown, the company should only acquire a cyber-insurance policy if the expected benefit exceeds the cost. The intersection of the benefit curve and the cost line is the threshold of attack probability that makes the company willing to buy cyber-insurance. As shown, the comparison between the policy bundles indicates that Policy B is preferable that provides the risk-neutral company with a larger net expected benefit of insurance, at any t above the threshold.

Apparently, choosing from predetermined cyber-insurance policy bundles is a simplification in the analysis. It is challenging to tailor cyber-insurance to the company. In practice as of today, premium and coverage often do not reflect actual risk level and dynamic exposure. Further research can be done to move from standardized cyber-insurance products to diversified and well-tailored policy bundles.

7. Conclusion

The rapid development of cyber-insurance shows the market is viable, but the impact of cyber-insurance on cybersecurity is not a settled issue. While more and more organizations adopt cyber-insurance, the need for organizations to find the best of both cybersecurity investment and cyber-insurance is increasing. It is imperative for organizations to understand these once distinct areas of investment and how the merging of the two has led to opportunities as well as increased uncertainty. When buying cyber-insurance reduces the organization's incentives for preventive cybersecurity investment, the attacker gains. Moreover, the cyber threat the organization faces is largely in the control of the attacker. Being breached may not be a random incident but the result of the attacker's calculation. Realizing how cyber-insurance changes the organization's cybersecurity investment, the attacker can launch cyber-attacks strategically to benefit from cyber-insurance.

This research focuses on a novel angle and sheds light on the overlooked issue of the effects of cyber-insurance from the attacker's perspective, and studies whether the attacker may manipulate and ultimately benefit from the cyber-insurance practice by playing the "hand of God". The model is a game between the attacker, whose strategy is to control attack probability, and the organization, whose strategy is to choose optimal cybersecurity portfolio comprising both cybersecurity investment and cyber-insurance. The theoretical analysis and the numerical example suggest that although cyber-insurance may be beneficial for the insured organization from a financial perspective, cyber-insurance may not always be the best from the cybersecurity perspective. Especially, the attacker may benefit from cyber-insurance with higher expected payoff from increased attack success rate resulting from the organization's reduced optimal cybersecurity investment. This paper contributes further by identifying the critical point (threshold) of such attack probability for organizations to switch to cyber-insurance practice, therefore significantly increasing the cyber attack payoffs. Plausible countermeasures against the attacker's manipulation of cyber-insurance provided by the development and modifications of the cyber-insurance market, the improved efficiency in cybersecurity investment, and the intervention of the government etc. are discussed.

For future research we plan to work on further extensions of the model. For example, self insurance can be included as an alternative to market insurance. In particular, this research considers a one-period model. In one-period economic models, all decisions and outcomes occur in a simultaneous instant. Thus, dynamic aspects such as the time value of money and the future increase in premium following claims are not considered directly. They are embedded in the model implicitly as part of private loss of the organization. Although the simplifying one-period framework serves the purpose of this research, future works on the dynamics of cybersecurity investment, cyber-insurance and changing incentives of game players will provide enriched analysis and more insights on cyber-insurance.

CRediT authorship contribution statement

Zhen Li: Formal analysis, Investigation, Writing – original draft, Methodology, Data curation. **Qi Liao:** Conceptualization, Writing – review & editing, Project administration.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

References

Abraham, K.S., Schwarcz, D.B., 2022. The limits of regulation by insurance. Indiana Law J. 98 (1), 214–274.

Aldasoro, I., Gambacorta, L., Giudici, P., Leach, T., 2022. The drivers of cyber risk. J. Financ. Stab. 60.

Awiszus, K., Knispel, T., Penner, I., Svindland, G., Voß, A., Weber, S., 2023. Modeling and pricing cyber insurance. Eur. Actuar. J. 13, 1–53.

Aziz, B., Suhardi, Kurnia, 2020. A systematic literature review of cyber insurance challenges. In: Proceedings of International Conference on Information Technology Systems and Innovation. ICITSI, Bandung, Indonesia, pp. 357–363.

Baker, T., 1996. On the genealogy of moral hazard. Tex. Law Rev. 75 (2), 237–292.

Baker, T., Shortland, A., 2022. The government behind insurance governance: Lessons for ransomware. Regul. Gov. 1–21.

Baker, T., Shortland, A., 2023. Insurance and enterprise: cyber insurance for ransomware. Geneva Pap. Risk Insur. - Issues Pr. 48, 275–299.

Bandyopadhyay, T., Mookerjee, V., 2019. A model to analyze the challenge of using cyber insurance. Inf. Syst. Front. 21, 301–325.

Bandyopadhyay, T., Mookerjee, V.S., Rao, R.C., 2009. Why IT managers don't go for cyber-insurance products. Commun. ACM 52 (11), 68–73.

Böhme, R., Laube, S., Riek, M., 2018. A fundamental approach to cyber risk analysis. Variance 12 (2), 161–185.

Böhme, R., Schwartz, G., 2010. Modeling cyber-insurance: Towards a unifying framework. In: Proceedings of the 9th Workshop on the Economics of Information Security. WEIS, Cambridge, MA.

Bolot, J.-C., Lelarge, M., 2008. Cyber insurance as an incentive for internet security. In: Proceedings of Workshop on the Economics of Information Security. WEIS, Hanover, NH, pp. 269–290.

Cartwright, A., Cartwright, E., MacColl, J., Mott, G., Turner, S., Sullivan, J., Nurse, J.R.C., 2023. How cyber insurance influences the ransomware payment decision: theory and evidence. Geneva Pap. Risk Insur. - Issues Pr. 48, 300–331.

Cunningham, B., Talesh, S.A., 2021. Uncle Sam RE: Improving cyber hygiene and increasing confidence in the cyber insurance ecosystem via government backstopping. Univ. Connect. Insur. Law J. 28, 1–84.

Dambra, S., Bilge, L., Balzarotti, D., 2020. SoK: Cyber insurance – technical challenges and a system security roadmap. In: Proceedinds of IEEE Symposium on Security and Privacy. SP, San Francisco, CA, pp. 1367–1383.

Ehrlich, I., Becker, G.S., 1972. Market insurance, self-insurance, and self-protection. J. Political Econ. 80 (4), 623–648.

Eisenbach, T.M., Kovner, A., Lee, M.J., 2021. Cyber risk and the U.S. financial system: A pre-mortem analysis. FRB N. Y. Staff. Rep. No. 909.

Enayaty-Ahangar, F., Albert, L.A., DuBois, E., 2020. A survey of optimization models and methods for cyberinfrastructure security. IISE Trans. 53 (2), 182–198.

Galina, S., Shetty, Nikhil, Walran, Jean, 2013. Why cyber-insurance contracts fail to reflect cyber-risks. In: Proceedings of 51st Annual Allerton Conference on Communication, Control, and Computing. Allerton, Monticello, IL, pp. 781–787.

Gordon, L.A., Loeb, M.P., 2002. The economics of information security investment. ACM Trans. Inf. Syst. Secur. 5 (4), 438–457.

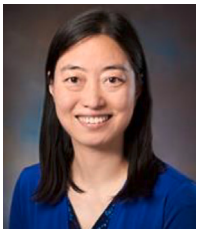
Gordon, L.A., Loeb, M.P., Lucyshyn, W., Zhou, L., 2015. Increasing cybersecurity investments in private sector firms. J. Cybersecur. 1 (1), 3–17.

Hayel, Y., Zhu, Q., 2015. Attack-aware cyber insurance for risk sharing in computer networks. In: Proceedings of the Sixth International Conference on Decision and Game Theory for Security. GameSec, London, UK, pp. 22–34.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., Stulz, R.M., 2018. What is the Impact of Successful Cyberattacks on Target Firms? Working Paper Series 24409, National Bureau of Economic Research.

Kesan, J.P., Majuca, R.P., Yurcik, W., 2005. Cyber-insurance as a market-based solution to the problem of cybersecurity. In: Proceedings of the 4th Workshop on the Economics of Information Security. WEIS, Cambridge, MA.

Khalili, M.M., Naghizadeh, P., Liu, M., 2018. Designing cyber insurance policies: The role of pre-screening and security interdependence. IEEE Trans. Inf. Forensics Secur. 13 (9), 2226–2239.
Khalili, M.M., Zhang, X., Liu, M., 2019. Effective premium discrimination for designing cyber insurance policies with rare losses. In: Proceedings of the 10th International Conference on Decision and Game Theory for Security. GameSec, Stockholm, Sweden, pp. 259–275.
Laszka, A., Panaousis, E., Grossklags, J., 2018. Cyber-insurance as a signaling game: Self-reporting and external security audits. In: Proceedings of the 9th Conference on Decision and Game Theory for Security. GameSec, Seattle, WA, pp. 508–520.
Lelarge, M., Bolot, J.-C., 2009. Economic incentives to increase security in the internet: The case for insurance. In: Proceedings of IEEE International Conference on Computer Communications. INFOCOM, Rio de Janeiro, Brazil, pp. 1494–1502.
Li, Z., Liao, Q., 2023. Does cyber-insurance benefit the insured or the attacker? – A game of cyber-insurance. In: Proceedings of the 14th Conference on Decision and Game Theory for Security. GameSec, Avignon, France.
Liao, Q., Li, Z., Striegel, A., 2012. Could firewall rules be public - a game theoretical perspective. J. Secur. Commun. Netw. 5 (2), 197–210.
Massaccia, F., Swierzbinskic, J., Williams, J., 2017. Cyberinsurance and public policy: Self-protection and insurance with endogenous adversaries. In: Proceedings of 16th Annual Workshop on the Economics of Information Security. WEIS, La Jolla, CA, pp. 1–38.
Mott, G., Turner, S., Nurse, J.R., MacColl, J., Sullivan, J., Cartwright, A., Cartwright, E., 2023. Between a rock and a hard(ening) place: Cyber insurance in the ransomware era. Comput. Secur. 128, 103162.
Nurse, J.R., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M., Creese, S., 2020. The data that drives cyber insurance: A study into the underwriting and claims processes. In: Proceedings of 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment. CyberSA, Dublin, Ireland, pp. 1–8.
Pal, R., Golubchik, L., 2010. Analyzing self-defense investments in internet security under cyber-insurance coverage. In: Proceedings of IEEE 30th International Conference on Distributed Computing Systems. ICDCS, Genoa, Italy, pp. 339–347.
Pal, R., Golubchik, L., Psounis, K., 2011. Aegis - a novel cyber-insurance model. In: Proceedings of Conference on Decision and Game Theory for Security. GameSec, College Park, Maryland, pp. 131–150.
Pal, R., Golubchik, L., Psounis, K., Hui, P., 2014. Will cyber-insurance improve network security? A market analysis. In: Proceedings of IEEE Conference on Computer Communications. INFOCOM, Toronto, Canada, pp. 235–243.
Pal, R., Golubchik, L., Psounis, K., Hui, P., 2018. The technologization of insurance: An empirical analysis of big data and artificial intelligence's impact on cybersecurity and privacy. ACM SIGMETRICS Perform. Eval. Rev. 45 (4), 7–15.
Panda, S., Woods, D.W., Laszka, A., Fielder, A., Panaousis, E., 2019. Post-incident audits on cyber insurance discounts. Comput. Secur. 87, 101593.
Parchomovsky, G., Siegelman, P., 2022. Third party moral hazard and the problem of insurance externalities. J. Leg. Stud. 51, 93–131.
Piromsopa, K., Klima, T., Pavlik, L., 2017. Designing model for calculating the amount of cyber risk insurance. In: Proceedings of Fourth International Conference on Mathematics and Computers in Sciences and in Industry. MCSI, Corfu, Greece, pp. 196–200.
Romanosky, S., Ablon, L., Kuehn, A., Jones, T., 2019. Content analysis of cyber insurance policies: how do carriers price cyber risk? J. Cybersecur. 5 (1), 1–19.
Shetty, N., Schwartz, G., Walrand, J., 2010. Can competitive insurers improve network security? In: Proceedings of the Third International Conference on Trust and Trustworthy Computing. TRUST, Berlin, Germany, pp. 308–322.
Talesh, S.A., 2018. Data breach, privacy, and cyber insurance: how insurance companies act as "compliance managers" for businesses. Law Soc. Inq. 43 (2), 417–440.
Talesh, S.A., Cunningham, B., 2021. The technologization of insurance: An empirical analysis of big data and artificial intelligence's impact on cybersecurity and privacy. Utah Law Rev. 2021 (5), 967–1027.
Tosh, D.K., Vakilinia, I., Shetty, S., Sengupta, S., Kamhoua, C.A., Njilla, L., Kwiat, K., 2017. Three layer game theoretic decision framework for cyber-investment and cyber-insurance. In: Proceedings of the 8th International Conference on Decision and Game Theory for Security. GameSec, Vienna, Austria, pp. 519–532.
Tsohou, A., Diamantopoulou, V., Gritzalis, S., Lambrinoudakis, C., 2023. Cyber insurance: state of the art, trends and future directions. Int. J. Inf. Secur. 22, 737–748.
Uuganbayar, G., Yautsiukhin, A., Martinelli, F., 2018. Cyber insurance and security interdependence: Friends or foes? In: Proceedings of 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment. Cyber SA, Glasgow, UK, pp. 1–4.
Uuganbayar, G., Yautsiukhin, A., Martinelli, F., Massacci, F., 2021. Optimisation of cyber insurance coverage with selection of cost effective security controls. Comput. Secur. 101 (102121), 1–21.
Wolff, J., 2022. Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks. The MIT Press.
Woods, D.W., Böhme, R., 2021. How cyber insurance shapes incident response: A mixed methods study. In: Proceedinds of the 20th Annual Workshop on the Economics of Information Security. WEIS, pp. 1–35.
Woods, D.W., Moore, T., 2020. Does insurance have a future in governing cybersecurity? IEEE Secur. Priv. 18 (1), 21–27.
Yang, Z., Lui, J.C., 2014. Security adoption and influence of cyber-insurance markets in heterogeneous networks. Perform. Eval. 74, 1–17.



Zhen Li is currently a John S. Ludington Endowed Professor of Economics in the Department of Economics and Management at Albion College. She received her Master's Degree and Ph.D. in Economics from Princeton University under the direction of Dr. Michael Woodford. She graduated with her Bachelor's Degree in International Economics from Peking University. Dr. Li conducted research on applied macroeconomics and international finance, in particular on international financial integrity and related policy issues. Dr. Li's recent research interests include inter-disciplinary research study on economics and game theory of computer networks and information security.

Qi Liao is currently a Professor of Computer Science at Central Michigan University (CMU). He received his M.S. and Ph.D. in Computer Science and Engineering (CSE) from the University of Notre Dame, and a B.S. and departmental distinction in Computer Science (minor in Mathematics) from Hartwick College, New York. Dr. Liao's research interests include computer security, machine learning, visual analytics, and economics/game theory at the intersection of network usage and cybersecurity. He received best paper awards at USENIX LISA, IEEE ICCCBDA, Emerald Literati Awards for Excellence for Information and Computer Security, IEEE VAST Challenge Award, winner of National Security Innovation Competition, Center for Research Computing Award for Computational Sciences and Visualization, and CMU College of Science & Engineering Award for Outstanding Research. Dr. Liao was a visiting research scientist at IBM Research, Argonne National Lab, and ASEE Fellow at U.S. Air Force Research Lab.