Astin Bulletin (2025), pp. 1–23
doi:10.1017/asb.2024.40

International Actuarial Association
Association Actuarielle Internationale

RESEARCH ARTICLE

Cybersecurity investments and cyber insurance purchases in a non-cooperative game

Tim J. Boonen[1], Yang Feng[2] and Zhiwei Tong[3]

[1]Department of Statistics and Actuarial Science, School of Computing and Data Science, The University of Hong Kong, Hong Kong, Hong Kong SAR, China
[2]School of Economics and Management, University of Science and Technology Beijing, Beijing 100083, China
[3]Department of Statistics and Actuarial Science, The University of Iowa, Iowa City, IA 52241, USA
Corresponding author: Yang Feng; Email: yangfeng_92@outlook.com

Received: 17 December 2023; **Revised:** 24 October 2024; **Accepted:** 16 December 2024

Keywords: Risk management; Nash equilibrium; cybersecurity; cyber insurance; network

Abstract

The growing concern over cyber risk has become a pivotal issue in the business world. Firms can mitigate this risk through two primary strategies: investing in cybersecurity practices and purchasing cyber insurance. Cybersecurity investments reduce the compromise probability, while cyber insurance transfers potential losses to insurers. This study employs a network model for the spread of infection among interconnected firms and investigates how each firm's decisions impact each other. We analyze a non-cooperative game in which each firm aims to optimize its objective function through choices of cybersecurity level and insurance coverage ratio. We find that each firm's cybersecurity investment and insurance purchase are strategic complements. Within this game, we derive sufficient conditions for the existence and uniqueness of Nash equilibrium and demonstrate its inefficiency. These theoretical results form the foundation for our numerical studies, allowing us compute firms' equilibrium decisions on cybersecurity investments and insurance purchases across various network structures. The numerical results shed light on the impact of network structure on equilibrium decisions and explore how varying insurance premiums influence firms' cybersecurity investments.

1. Introduction

Cyber risk has emerged as a major concern across various sectors and industries, including healthcare, finance, and technology, due to the increase in both frequency and financial consequences, which are the two pillars of the underlying losses. Over the past decade, the number of cyberattacks has tripled in terms of frequency, with the financial services sector being the primary target.[1] As indicated in a report by IBM Security (2024), the number of data breaches and cybersecurity incidents has increased with the growing number of devices connected to the internet, especially during the COVID-19 pandemic years.[2] In terms of severity, the same report also indicates that the global average cost of a data breach has soared to an all-time high of \$4.45 million, which represents a 15% increase over three years.

Some high-profile cases illustrate the devastating impacts of cyber incidents. A report by the Cybersecurity and Infrastructure Security Agency (CISA) for the year 2020 provides an in-depth breakdown of the financial implications and demographic impacts of significant cybersecurity incidents,[3] and

[1] See the article by the International Monetary Fund (IMF), available at https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability.

[2] See the 2024 report by IBM Security titled "Cost of Data Breach Report 2024" available at https://www.ibm.com/reports/data-breach.

[3] See the report by CISA titled "2020 Year in Review" available at https://www.cisa.gov/resources-tools/resources/cisa-2020-year-review.

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

the same agency provides ongoing updates regarding the most substantial incidents to date in another report.[4] In 2022, mobile communications company T-Mobile announced a settlement following a data breach that occurred in early 2021, impacting approximately 77 million people. In 2023, Microsoft AI researchers accidentally exposed 38 terabytes of sensitive data. In April 2024, over 4.1 billion records of 600 million users of Discord, a popular gaming platform, were breached and were sold over the internet. These incidents highlight the far-reaching consequences of cyberattacks, which extends beyond immediate financial losses. As Agrafiotis *et al*. (2018) point out, the repercussions also include long-term reputation damage, business disruptions, lost opportunities, and eroded trust.

IT systems foster interconnectivity among users, and this interconnected nature of IT systems acts as a double-edged sword, greatly enhancing productivity while simultaneously contributing to the spread of cyber threats. A report by the European Systemic Risk Board (2020) highlights that in an increasingly digitalized world where critical infrastructure, businesses, and individuals heavily depend on interconnected networks, the potential for cyber threats to proliferate and intensify is significant.[5] On a separate note, Eisenbach *et al*. (2022) conduct an analysis of the financial system, which is heavily reliant on the wholesale payments network and find that cyberattacks may significantly disrupt the operation of the financial system. As IT systems grow more interdependent, a breach or disruption in one system can rapidly spread to others, making it difficult to contain the scope and severity of cyber incidents.

In the face of challenges brought about by cyber risk, firms and organizations need to thoroughly evaluate the costs and benefits of implementing robust cybersecurity practices, such as advanced firewalls and intrusion detection systems. These cybersecurity practices can mainly help to reduce the frequency of cyberattacks. Complementing these practices is the purchase of cyber insurance, which reduces exposure at compromise and hence mitigates the financial consequences of cyberattacks. Cyber insurance has emerged as a powerful and popular tool for managing cyber risk. As discussed by the US Government Accountability Office (2020), cyber insurance typically covers expenses due to common cyber incidents, including data breaches, ransomware attacks, and business interruptions resulting from cyberattacks.[6]

In our work, we investigate the decisions of interconnected firms faced with the choice between investing in cybersecurity practices and purchasing cyber insurance. Under our framework, the more a firm invests in cybersecurity, the higher its cybersecurity level becomes, and the less likely it is to be compromised when an infection reaches it, *ex ante*. A firm can also buy proportional cyber insurance to receive *ex post* reimbursement if a cyber loss occurs. In a network of interconnected firms, in which a firm's own cybersecurity level impacts the overall resilience of the entire network, firms' decisions interact with each other. Naturally, game theory becomes a suitable tool for studying cyber risk decision-making problems. We focus on a pure-strategy Nash equilibrium framework, where each firm aims to optimize its own objective function through decisions on cybersecurity level and insurance coverage. We characterize the equilibrium decisions and find that each firm's cybersecurity investment and insurance purchase are strategic complements. To be more specific, keeping everything else unchanged, the more a firm's insurance coverage, the less it invests in cybersecurity, and vice versa. We derive sufficient conditions for the existence and uniqueness of equilibrium, which allows us to conduct extensive numerical studies to compute the equilibrium decisions and illustrate the impacts of network structure and insurance premiums on the equilibrium decisions. We also establish two results that show the inefficiency of the Nash equilibrium. The first result, established under certain homogeneity and symmetry assumptions, indicates that firms tend to underinvest in the Nash equilibrium, which leads to less beneficial outcomes for all firms collectively. The second result, established under mild conditions, shows that the Nash equilibrium is not Pareto efficient.

[4] See the latest list of incidents by CISA available at https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-06/240607_Significant_Cyber_Events.pdf?VersionId=E3Y46OOqM9GsO4KNWizmvg7aA2NYZ2a6.

[5] See the 2020 report by European Systemic Risk Board titled "Systemic Cyber Risk" available at https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

[6] See the 2022 report by US Government Accountability Office titled "Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks" available at https://www.gao.gov/products/gao-22-104256.

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

In order to derive these findings, we make several foundational assumptions. First, insurance is assumed to be of a proportional type, meaning that the insured pays a premium proportional to the coverage ratio, and the pricing is assumed to be linear with exogenous premium rates. This assumption is consistent with the framework employed by Boonen and Liu (2022) in a general insurance context. Additionally, we examine expected utility preferences of firms. The dis-utility or cost associated with increasing cybersecurity practices is modeled using a convex cost function, reflecting the realistic scenario that additional cybersecurity investments yield diminishing benefits as the cybersecurity level increases. This cost function is assumed to be separable from the expected utility function, allowing for a clearer analysis of its impact. Furthermore, while realistically cybersecurity practices can affect both the frequency and severity of losses, our study focuses solely on their impact on the frequency of cyber incidents. This restriction, although a simplification, enables us to provide a more focused and tractable analysis, serving as a foundation for future research that might incorporate the impact on severity as well. Besides, among the numerous network contagion models, we adopt the random attack model detailed by Acemoglu *et al*. (2016), where a firm's compromise probability can be decomposed into one part concerning its own cybersecurity level and another concerning others. This model assumes that during any given time period, there is exactly one cyber incident, in which an attacker randomly selects a firm within the network as the initial target. If this firm is breached, the contagion can spread to other connected firms. This model is elegantly simple, yet captures the essence of contagion and allows for a manageable analysis.

1.1 Literature review

This subsection provides a curated and focused literature review of the extensive research on cyber risk with a concentration on those studies most pertinent to our work. Driven by rising concerns regarding cyber risk, recent years have seen a significant uptick in research on this topic. Eling (2020) and Awiszus *et al*. (2023) review the academic literature on cyber risk and cyber insurance and call for more research to understand the characteristics in the distribution of cyber risk, including its frequency, severity, and dependency structure. Eling *et al*. (2021) show the historical evolution of cybersecurity research as well as the current state of cyber risk management. They point out the critical challenge of incorporating cyber risk into broader enterprise risk management strategies. Dacorogna and Kratz (2023) further provide a comprehensive discussion on the risk management of cyber risk, including the implications for actuaries.

A potential solution to cyber risk is insurance, which provides essential services and funding to help resume operations quickly and is thus important for recovery from cyberattacks. However, conflicting views exist on whether cyber insurance exacerbates the cyber crisis by potentially encouraging ransom payments. Some argue that it actually worsens the crisis, with reports suggesting that organizations with such policies are increasingly targeted by ransomware gangs. See Mott *et al*. (2023) for a more in-depth discussion.

Driven by increasing demand and dynamic risk exposures, the cyber insurance market continues to mature; see, for example, the survey by Munich Re (2024).[7] Related papers include Biener *et al*. (2015), who explore the insurability of cyber risk through an empirical analysis, and Marotta *et al*. (2017), who provide an in-depth overview of the cyber insurance market, examining both supply and demand perspectives. More recently, Awiszus *et al*. (2024) study the design of systemic cyber risk obligations and measure the corresponding systemic risk contributions of individual policyholders.

In the face of cyber risk, firms may purchase cyber insurance to hedge against losses due to cyberattacks, and/or they may invest in cybersecurity practices to reduce the likelihood of being breached or to constrain the scope of breaches. There has been extensive literature on cyber risk decision problems, for which a comprehensive review can be found in Marotta *et al*. (2017) and Awiszus *et al.* (2023). In particular, a common theme in existing works has focused on how to design or price insurance contracts

[7] See the 2024 survey by Munich Re titled "Global Cyber Risk and Insurance Survey 2024" available at https://www.munichre.com/en/insights/cyber/global-cyber-risk-and-insurance-survey.html.

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

to mitigate moral hazard and asymmetric information or the marketability of cyber insurance; see, for example, Pal (2012), Pal *et al*. (2014, 2019), Khalili *et al.* (2017), and Xiang *et al.* (2024). For analytical tractability, a majority of cyber decision problems are performed with rather stylized network structures or are derived from a rather *ad hoc* scheme where the probability of a firm being compromised depends on the average security level of the other firms in the network; see, for example, Ogut *et al*. (2005) and Shetty *et al*. (2010).

Our work contributes to the literature by studying interactions among firms whose decisions depend on each other due to the contagious nature of cyber risk. Within this framework, game-theoretic approaches naturally become a handy tool. Along this stream of literature, the two works most related to ours are Acemoglu *et al*. (2016) and Nagurney and Shukla (2017). Acemoglu *et al.* (2016) also investigate the Nash equilibrium and compare it with the social optimum, exploring how a novel set of network centrality measures influences these investment levels. Nagurney and Shukla (2017) explore three distinct game-theoretic models of cybersecurity investments in various non-cooperative and cooperative situations: the Nash equilibrium model, the Nash bargaining model, and the system optimization model. To properly study the game between firms and their decisions, it is necessary to use an appropriate contagion model that reflects their influence on each other. We adopt the model of Acemoglu *et al.* (2016), which provides a natural factorization of the probability of a firm being eventually compromised into a product of its own decision and the decisions of others. This model is more appropriate than the one employed by Nagurney and Shukla (2017), which was proposed by Shetty *et al.* (2010). The latter assumes that a firm’s likelihood of being compromised is determined by its own cybersecurity level and the average security level of all firms, without considering the intricacies of network structure. Both works do not consider the possibility of purchasing cyber insurance as a loss mitigation tool. An important addition in our work to these two main references is the incorporation of cyber insurance as a decision variable alongside cybersecurity investment. This novel aspect allows us to explore the interplay between investment in cybersecurity and the purchase of insurance.

There are multiple other works within the game-theoretical framework that also address cyber risk decision problems, yet their focuses differ from ours. For example, both Ogut *et al*. (2005) and Shetty *et al.* (2010) consider decision-making problems involving both cyber insurance and cybersecurity. The focus of Ogut *et al*. (2005) is on the implications of interdependence on decision-making, and the focus of Shetty *et al*. (2010) is on the marketability of insurance and the competition between insurers. Some studies have sparked debates on whether the provision of cyber insurance can incentivize cybersecurity investment or actually exacerbate a cyber crisis by potentially encouraging ransom payments. For example, Yang and Lui (2014) and Schwartz and Sastry (2014) both analyze the optimal decision of firms on cybersecurity in environments both with and without cyber insurers. Yang and Lui (2014) employ a Bayesian network game to capture situations in which firms in heterogeneous networks have only local information. They find that cyber insurance is more likely to be a beneficial incentive for firms with higher degrees in these networks. On the other hand, Schwartz and Sastry (2014) study the Nash equilibrium between firms and find that in the presence of cyber insurers, equilibrium network security is lower than if no cyber coverage is available. A recent paper by Zeller and Scherer (2023) studies a Stackelberg game in which firms seek to minimize specific risk measures. In this game, an insurer acts as the leader and provides both insurance and risk mitigation services.

We conclude the literature review with some recent developments in actuarial modeling of cyber risk. Recognizing the unique high-dependency characteristic of cyber risk, Peng *et al*. (2018) use copulas to model the multivariate dependence exhibited by real-world cyberattack data. Jevtić and Lanchier (2020) propose a tree-based model for the spread of infection and investigate the distribution of aggregate losses due to breaches. Da *et al*. (2021), Xu and Hua (2019), and Zhang *et al*. (2023) propose models that capture the unique cybersecurity features of fog networks and address the important issue of cybersecurity risk pricing. Fahrenwaldt *et al*. (2018) explore the implications of network structure on the pricing of cyber insurance contracts, and Hillairet *et al.* (2022) introduce a model that takes network structure into consideration to capture the cyber-contagion process, illustrating the impact of a massive cyberattack on

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

an insurance portfolio. A recent study of Braun *et al.* (2023) explores the feasibility and challenges of transferring cyber risk through insurance-linked securities. By analyzing the preferences of both insurers and investors under various sources of risk, they emphasize the importance of building mature cyber risk models.

The rest of the paper is organized as follows. In Section 2, we show the optimal decisions for a firm from a stand-alone perspective. Section 3 extends this to the setting with competition in a network. Section 4 presents the conditions for the existence and uniqueness of Nash equilibrium and discusses the inefficiency of Nash equilibrium. Section 5 conducts numerical studies to examine firms' equilibrium decisions under various network structures and explore the interplay between the two decision variables. Section 6 provides concluding remarks, and the proofs are delegated to the Appendix.

2. A firm in isolation

We start our study by considering a firm operating as an isolated entity. Our goal is to characterize the firm's decisions regarding cybersecurity investment and insurance purchase. In the next section, we will extend our analysis to a network of firms where their decisions influence each other.

Denote by Y the indicator of the firm being compromised in a cyber incident, and by $p = P(Y = 1)$, the compromise probability. For this firm to be compromised, the infection must first reach the firm, and then the firm's IT system must also lack the immunity to the infection. Therefore, the compromise probability, p, can be factorized into the product of two terms:

$$p = \tilde{p}\,(1 - q)\,, \tag{2.1}$$

where $\tilde{p}$ represents the probability of infection reaching the firm and q is the probability that the firm is immune to the infection. This probability q can be interpreted as the cybersecurity level of the firm's IT system. We assume that $\tilde{p}$ does not depend on q, ignoring the externality whereby less protected firms might become more attractive targets for attackers. This simplifies the setup and avoids the need to impose an *ad hoc* dependency of $\tilde{p}$ on q.

Let W denote the revenue the firm derives if it remains uncompromised, and L denote the loss at compromise. We allow both W and L to be random variables and require $0 \leq L \leq W$. Throughout the paper, we assume that neither W nor L is degenerate at 0, which rules out the possibility of zero cyber risk. The firm has two ways of mitigating the risk of being compromised in cyber incidents: (i) invest in cybersecurity practices to enhance the cybersecurity level q, and (ii) purchase cyber insurance to get compensated for part of the loss L. In practice, cybersecurity practices can mitigate both the likelihood and severity of losses. However, our study specifically limits the benefits of these practices to reducing the likelihood alone. Denote the cost (or dis-utility) of establishing a cybersecurity level of q as $c(q)$. Naturally, we require the function $c(\cdot)$ to be twice differentiable, strictly increasing, and strictly convex, and also require it to satisfy the boundary condition $c(0) = 0$.

In this paper, we consider a proportional insurance scheme in which an insurer covers a proportion, denoted as $a \in [0, 1]$, of the loss. Proportional insurance is often attractive, as it helps to retain tractable outcomes. Reinsurance is an important application for proportional indemnities, since "this form of reinsurance is popular in almost all insurance branches, particularly due to its conceptual and administrative simplicity," as argued by Albrecher *et al.* (2017). In homeowners insurance, proportional insurance is popular as it is related to the so-called coinsurance clause in the United States. This means that when a house is insured, a minimal proportion of the house value needs to be covered; see, for example, Boonen and Liu (2022). Let $\pi > 0$ be the premium for full coverage, corresponding to $a = 1$. We treat π as exogenously given for two main reasons. First, the insurer may not constantly observe a firm's security level in practice, and the insurance price may not instantly reflect any changes in a firm's security level. More importantly, the focus of this work is a non-cooperative game between firms in a network. Making the premium depend on cybersecurity levels would require a separate study in which

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

the insurer also becomes an active player, as the insurer needs to adjust the premium as firms adjust their cybersecurity levels.

Under a linear pricing scheme, the cost of insurance for a coverage ratio of a is $a\pi$. It is up to the firm to determine a, which reflects the decision on how much of the loss the firm wants to insure. Cyber risk, by its nature, is highly unpredictable and entails an enormous amount of uncertainty. Unlike other popular insurable risk, quantifying the actual losses in a cyber incident is challenging. Therefore, proportional insurance can be a useful contract to share the costs between the insurer and policyholder in case of risk misspecification.

Using a utility function $U:\mathbb{R}_+ \mapsto \mathbb{R}$ to reflect the firm's risk aversion, the objective function of this firm, defined as the expected utility of cash inflow at the end of the period minus the cybersecurity investment and insurance purchase cost at the beginning, is given by:

$$u\left(a,q\right) = \mathbb{E}\left[U\left(W-(1-a)LY\right)\right] - c\left(q\right) - a\pi, \quad \text{for } \left(a,q\right) \in [0,1]^2\,. \tag{2.2}$$

This can be written as:

$$u(a,q) = \tilde{p}\left(1-q\right)\mathbb{E}\left[U\left(W-(1-a)L\right)\right] + \left(1-\tilde{p}\left(1-q\right)\right)\mathbb{E}\left[U\left(W\right)\right] - c\left(q\right) - a\pi. \tag{2.3}$$

The firm aims to maximize $u(a,q)$ through choices of insurance coverage ratio a and cybersecurity level q, over $(a,q) \in [0,1]^2$. Throughout the paper, all utility functions are assumed to be twice differentiable, strictly increasing, and strictly concave. Note that the functional form of u above is endowed with a quasi-linearity property; the utility function is additive in the time-0 measurable cash payments $c\left(q\right)+a\pi$, while expressing risk aversion through strict concavity.

2.1 The optimal insurance coverage ratio given the cybersecurity level and vice versa

Recall from (2.1) and the discussions around it that the probability of infection reaching a firm, $\tilde{p}$, does not concern the firm's own cybersecurity level. Then, it is clear that when $\tilde{p}=0$, this firm faces no cyber threats at all and, therefore, from (2.3), it will not invest in cybersecurity or purchase cyber insurance. Thus, in this subsection, we assume $\tilde{p}>0$, which is the more interesting and non-trivial situation.

The following lemma shows the uniqueness of the maximizer of u given q. We also identify conditions for the maximizer to be at the boundaries or satisfy the first-order condition.

Lemma 2.1 *For any fixed $q \in [0,1]$, there is a unique $a \in [0,1]$ that maximizes $u\left(a,q\right)$ defined in (2.2). Let*

$$\hat{a}\left(q\right) = \arg\max_{a\in[0,1]} u\left(a,q\right). \tag{2.4}$$

Denote by $\tilde{a}(q)$, for $q \in [0,1)$, the solution to the following equation for $\tilde{a} \in [0,1]$ if it exists:

$$(1-q)\tilde{p}\mathbb{E}[U'(W-(1-\tilde{a})L)L] = \pi. \tag{2.5}$$

Depending on the value of π, three cases are possible:

1. *If $\pi \geq \tilde{p}\mathbb{E}\left[U'\left(W-L\right)L\right]$, then $\hat{a}\left(q\right)=0$ for any $q \in [0,1]$.*
2. *If $\tilde{p}\mathbb{E}\left[U'\left(W\right)L\right] < \pi < \tilde{p}\mathbb{E}\left[U'\left(W-L\right)L\right]$, then*

$$\hat{a}\left(q\right) = \begin{cases} \tilde{a}\left(q\right), & \text{if } q \in \left[0, 1-\frac{\pi}{\tilde{p}\mathbb{E}\left[U'(W-L)L\right]}\right); \\ 0, & \text{if } q \in \left[1-\frac{\pi}{\tilde{p}\mathbb{E}\left[U'(W-L)L\right]}, 1\right]. \end{cases}$$

3. *If $\pi \leq \tilde{p}\mathbb{E}\left[U'\left(W\right)L\right]$, then*

$$\hat{a}\left(q\right) = \begin{cases} 1, & \text{if } q \in \left[0, 1-\frac{\pi}{\tilde{p}\mathbb{E}\left[U'(W)L\right]}\right]; \\ \tilde{a}\left(q\right), & \text{if } q \in \left(1-\frac{\pi}{\tilde{p}\mathbb{E}\left[U'(W)L\right]}, 1-\frac{\pi}{\tilde{p}\mathbb{E}\left[U'(W-L)L\right]}\right); \\ 0, & \text{if } q \in \left[1-\frac{\pi}{\tilde{p}\mathbb{E}\left[U'(W-L)L\right]}, 1\right]. \end{cases}$$

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

Lemma 2.1 tates that, given a cybersecurity level $q \in [0, 1]$, the optimal insurance coverage ratio is unique, defining the function $\hat{a}\left(\cdot\right)$. Therefore, the problem with two decision variables essentially reduces to a problem with one decision variable. Namely, once the optimal cybersecurity level $\hat{q}$ is determined, the optimal coverage ratio $\hat{a}\left(\hat{q}\right)$ follows accordingly.

Lemma 2.1 also shows that there are three distinct cases where the function $\hat{a}\left(\cdot\right)$ takes on different forms. These cases are decided by the range of the full-coverage insurance premium, π, and some other factors including the probability of infection reaching the firm, $\tilde{p}$. In later sections where a network of firms is studied, $\tilde{p}$ also depends on the cybersecurity levels of other firms. As a result, the optimal coverage ratio of each firm depends on the decisions made by other firms.

Taking a closer look at the three cases reveals that, if π is excessively high, then regardless of the cybersecurity level, the firm will not purchase any insurance coverage. Otherwise, the optimal coverage ratio $\hat{a}\left(q\right)$ given q may be 0, 1, or $\tilde{a}\left(q\right)$, which solves the first-order condition (2.5). The case when $\tilde{a}\left(q\right)$ is achieved only occurs when the cybersecurity level is strictly less than 1, that is, $q < 1$. This is quite intuitive because when $q = 1$, the firm is completely immune to any infection, which immediately implies that $\hat{a}\left(1\right) = 0$.

For q away from 0, applying the implicit function theorem to (2.5) yields

$$\tilde{a}'\left(q\right) = -\frac{\mathbb{E}\left[U'\left(W - \left(1 - \tilde{a}\left(q\right)\right)L\right)L\right]}{\mathbb{E}\left[-U''\left(W - \left(1 - \tilde{a}\left(q\right)\right)L\right)L^2\right]}\frac{1}{1-q} < 0. \tag{2.6}$$

It is also straightforward to verify that $\hat{a}\left(q\right)$ is continuous in $q \in [0, 1]$ in all three cases. This leads to the following conclusion in Proposition 2.1, which shows that the more a firm invests in cybersecurity, the less insurance coverage it purchases.

Proposition 2.1 *The function $\hat{a}\left(\cdot\right)$, defined in (2.4), is continuous and decreasing in $q \in [0, 1]$.*

In the above analysis, we take the cybersecurity level as fixed and study the optimal insurance coverage ratio. We can also fix the coverage ratio and study the optimal cybersecurity level in a similar manner. Notice that the objective function (2.3) is strictly concave in q due to the strict convexity of the cost function $c(\cdot)$. Therefore, given a coverage ratio $a \in [0, 1]$, the optimal cybersecurity level is unique, defining a function. This function is decreasing also due to the strict convexity of $c(\cdot)$. We present the following proposition to characterize this function.

Proposition 2.2 *For any fixed $a \in [0, 1]$, there is a unique $q \in [0, 1]$ that maximizes u(a,q) defined in (2.2). Let*

$$\hat{q}(a) = \arg\max_{q \in [0,1]} u(a, q).$$

Then, $\hat{q}(a)$ is decreasing in a.

Propositions 2.1 and 2.2 jointly show that investment in cybersecurity and purchase of insurance are strategic complements. That is, the greater a firm's insurance coverage is, the less it invests in cybersecurity, and vice versa.

2.2 Reducing to a single-variable decision problem

In the previous subsection, we have studied the problem of maximizing $u(a, q)$ while taking q as fixed, that is, determining the optimal insurance coverage ratio, $\hat{a}(q)$. In this notation, $\hat{a}$, we use the hat to indicate the optimal decision. With a slight abuse of notation, we add a hat above u so that $\hat{u}(q)$ represents the firm's bivariate objective function $u(a, q)$ with a set to the unique optimal coverage ratio $\hat{a}(q)$. That is,

$$\hat{u}\left(q\right) = u\left(\hat{a}\left(q\right), q\right) = \mathbb{E}\left[U\left(W - \left(1 - \hat{a}\left(q\right)\right)LY\right)\right] - c\left(q\right) - \hat{a}\left(q\right)\pi, \quad \text{for } q \in [0, 1]. \tag{2.7}$$

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

We intentionally write the univariate objective function $\hat{u}(q) = u\left(\hat{a}(q), q\right)$ to distinguish it from the original bivariate $u(a, q)$. Maximizing $u(a, q)$ via the choice of $(a, q) \in [0, 1]^2$ is equivalent to maximizing $\hat{u}(q)$ via the choice of $q \in [0, 1]$.

Note that $\hat{u}(\cdot)$ is a continuous function on the compact domain [0, 1], and so a maximum always exists. It is easy to find the optimal cybersecurity level q and the corresponding maximum value of the objective function numerically. Despite so, in later sections, we will explore a network of firms and study their interactions. At that point, we often need $\hat{u}(\cdot)$ to satisfy certain concavity conditions so that a Nash equilibrium exists. For that purpose, we present the following lemma to characterize the concavity of $\hat{u}(\cdot)$.

Lemma 2.2 *Consider the function $\hat{u}(\cdot)$ defined in (2.7).*

1. *If $\pi \geq \tilde{p}\mathbb{E}\left[U'(W-L)L\right]$, then $\hat{u}(\cdot)$ is concave.*
2. *If $\pi < \tilde{p}\mathbb{E}\left[U'(W-L)L\right]$, then $\hat{u}(\cdot)$ is concave under the extra condition that*

$$c''(q) > \frac{\pi}{R}\frac{1}{(1-q)^2}, \quad \text{for } q \in [0, 1], \tag{2.8}$$

where R is a positive coefficient defined as:

$$R = \inf_{a\in[0,1]} \frac{\mathbb{E}\left[-U''(W-(1-a)L)L^2\right]}{\mathbb{E}\left[U'(W-(1-a)L)L\right]}. \tag{2.9}$$

A high convexity of the cost function reflects the realistic scenario that as the cybersecurity level q increases, the marginal cost of further enhancing the cybersecurity level sharply rises. The coefficient R, introduced in (2.9), is related to the Arrow–Pratt risk aversion coefficients and depends only on the utility function, as well as the revenue and loss distributions, as illustrated in the following examples. This coefficient plays an important role in the conditions we derive in later sections to ensure the existence and uniqueness of Nash equilibrium.

Example 2.1 *(With deterministic revenue and loss). Suppose the revenue W without being compromised and the loss L at compromise are both deterministic. Considering the exponential utility with constant absolute risk aversion $\rho > 0$, that is,*

$$U(w) = \frac{1-e^{-\rho w}}{\rho}, \quad w \geq 0, \tag{2.10}$$

the coefficient R is given by:

$$R = \rho L.$$

Considering the power utility function with constant relative risk aversion $\eta > 0$, that is,

$$U(w) = \begin{cases} \frac{w^{1-\eta}}{1-\eta}, & \text{if } \eta \neq 1, \\ \ln(w), & \text{if } \eta = 1, \end{cases}$$

for $w > 0$, the coefficient R is given by:

$$R = \inf_{a\in[0,1]} \frac{-U''(W-(1-a)L)L}{U'(W-(1-a)L)} = \inf_{a\in[0,1]} \frac{\eta L}{W-(1-a)L} = \eta\frac{L}{W}.$$

With both utility functions, R is proportional to the risk aversion coefficients.

Example 2.2 *(With random revenue and loss). Suppose the revenue W without being compromised is distributed as the exponential distribution with a mean of 1, and the loss L at compromise is a fixed ratio $\theta \in (0, 1)$ of W. Considering the exponential utility in (2.10), we can verify that*

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

$$\mathbb{E}\left[-U''\left(W-(1-a)L\right)L^2\right]=\frac{2\rho\theta^2}{\left[\rho\left(1-(1-a)\theta\right)+1\right]^3},$$
$$\mathbb{E}\left[U'\left(W-(1-a)L\right)L\right]=\frac{\theta}{\left[\rho\left(1-(1-a)\theta\right)+1\right]^2}.$$

Consequently, the coefficient R is given by:

$$R=\inf_{a\in[0,1]}\frac{2\rho\theta}{\rho\left(1-(1-a)\theta\right)+1}=\frac{2\rho}{\rho+1}\theta.$$

3. The network model for the spread of infection

The analysis of a single firm's decisions in the previous section lays the foundation for the analysis of the game involving multiple firms in the following sections. To this end, we need to employ an appropriate contagion model that reflects their influence on each other. We extend the idea of the factorization in (2.1), which leads to the formal introduction of the random attack model by Acemoglu *et al*. (2016) below. This model provides a tractable decomposition of each individual compromise probability into an own effect and an externality.

Consider d firms forming a network, each represented by an index from $\{1,\ldots,d\}$. Following Acemoglu *et al*. (2016), we assume that there is only one incident during the period, initiated when a blind attacker randomly targets one of these d firms for an attack. In other words, each firm is attacked with an equal probability of $\frac{1}{d}$.[8] The cybersecurity system of the initially targeted firm is either immune or susceptible to this specific attack. If the system is immune, nothing happens. Otherwise, the firm becomes compromised, and the infection spreads from this firm to its connections, or "neighbors." Once a firm is compromised, it immediately propagates the infection to all neighbors, and these neighbors become susceptible.[9] If a firm, say firm i, is immune to the infection, which occurs with probability q_i, representing its cybersecurity level, it remains uncompromised. This propagation continues from compromised firms to their neighbors and stops when no new firms are compromised, and all these events occur instantaneously. In other words, a single directly targeted firm (node) is sampled uniformly from a given graph, and its likelihood of being compromised depends on its cybersecurity level. Nodes that are linked to any compromised nodes constitute a subgraph of susceptible nodes. The likelihood that these nodes will be compromised after becoming susceptible also depends on their cybersecurity levels.

Using the same notations as in Section 2, but adding a subscript i to indicate firm i, p_i represents the probability that firm i is eventually compromised, $\tilde{p}_i$ represents the probability of infection reaching firm i, that is, firm i becomes susceptible, and q_i, as just explained, represents firm i's cybersecurity level and the probability that firm i is immune to the infection. For convenience, we write $q=(q_1,\ldots,q_d)$, and q_{-i} is the $(d-1)$-dimensional vector which is q with the ith dimension removed. With these notations introduced, we further illustrate the model we adopt with the following example.

Example 3.1 *In this example, we illustrate the spread of infection within a network of five firms, as plotted in Figure 1. Within this specific network, we derive an explicit expression for the probability of infection reaching firm 1, as shown below:*

[8] We can extend the model to allow for a probability of a cyberattack occurring during the period. In this case, there could be one or no initial cyberattack in the network, and we could assume the probability of any attack during the period is $\lambda\in(0,1]$, which may not necessarily be 1. If we still assume that the attacker randomly selects one firm to target, conditional on an attack occurring, then the probability of infection reaching any firm is scaled by λ. To avoid confusion by introducing a new parameter λ, we adhere to the approach of Acemoglu *et al*. (2016) and set $\lambda=1$.

[9] In this paper, we adopt the contagion model from Acemoglu *et al*. (2016), which assumes that the spread probability from one compromised node to all its neighbors is 1. For other cyber risk models with spread probabilities allowed to be below 1, see Da *et al*. (2021), Hillairet *et al*. (2022), and Zhang *et al*. (2023), among others.

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

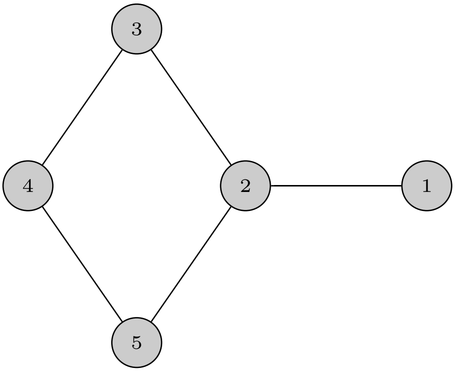

Figure 1. *This figure depicts a network of five firms, where firms 2 to 5 form a ring and firm 1 is connected only to firm 2.*

$$\tilde{p}_1 = \frac{1}{5} + \frac{1}{5}(1-q_2) + \frac{1}{5}(1-q_3)(1-q_2)(1+(1-q_4)(1-q_5))$$
$$+\frac{1}{5}(1-q_4)(1-q_2)((1-q_3)+(1-q_5)) + \frac{1}{5}(1-q_5)(1-q_2)(1+(1-q_4)(1-q_3)).$$

The right-hand side of the above equation consists of multiple terms, each representing a different scenario in which the infection could reach firm 1. The first term represents the probability of firm 1 being directly attacked by the attacker. The subsequent terms calculate the probabilities that the infection, initially affecting a different firm, eventually spreads to firm 1 through various network paths. For example, the third term calculates the probability that firm 3 is initially compromised, and then the infection reaches firm 2 either directly or via firms 4 and 5, before finally spreading to firm 1.

From the above discussion, it can be seen that the probability of firm i being the initial target in the cyber incident has been incorporated into $\tilde{p}_i$. Moreover, within a network of firms, the probability $\tilde{p}_i$ does not depend on the cybersecurity level of firm i itself, but on those of the other firms, for which we will write $\tilde{p}_i = \tilde{p}_i\left(q_{-i}\right)$. This will be violated if the assumption stated above that the attacker randomly selects a firm as the initial target is removed. Then, the probability of firm i being compromised in a network equals $\tilde{p}_i\left(q_{-i}\right)$ times the probability that it is not immune to this infection, which depends on the security level of firm i itself. This leads to the following decomposition:

$$p_i = (1-q_i)\,\tilde{p}_i\left(q_{-i}\right), \tag{3.1}$$

which is presented as Proposition 1 of Acemoglu *et al*. (2016). The probability $\tilde{p}_i$ decreases with the security levels of the other firms, with the partial derivatives given by:

$$\frac{\partial \tilde{p}_i\left(q_{-i}\right)}{\partial q_j} = -Q_{ij} \leq 0, \tag{3.2}$$

where Q_{ij} is the probability of infection reaching firm i via a path that contains firm j, conditional on firm j being susceptible. This is presented as Proposition 2 of Acemoglu *et al*. (2016). Applied to Example 3.1, taking the partial derivative of $\tilde{p}_1\left(q_{-1}\right)$ with respect to q_2 yields $-Q_{12}$, where Q_{12} is the probability of infection reaching firm 1 via a path that contains firm 2, conditional on firm 2 being susceptible.

We adopt the model of Acemoglu *et al*. (2016) because the decomposition in (3.1) essentially rephrases (2.1) within the context of a network of firms, based on the fundamental concept of conditional probability. Other game-theoretical studies of cyber risk, such as Shetty *et al.* (2010) and Nagurney and Shukla (2017), also use a contagion model. In these models, the probability of a firm eventually being compromised decomposes into an own effect and an externality. However, the term $\tilde{p}_i\left(q_{-i}\right)$ in their model depends on the average security levels of the other firms, rather than the detailed contagion mechanism proposed by Acemoglu *et al.* (2016).

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

4. Equilibrium cybersecurity investments and insurance purchases

4.1 Nash equilibrium

A single firm's decision on cybersecurity investment depends on the probability of infection reaching it, as seen in Section 2. This probability, in turn, depends on the cybersecurity levels of the other firms in the network, which is discussed around (3.1). Therefore, firms' decisions on their cybersecurity investments interact with each other. There could be different types of interactions among firms in a network, and in this work, we study a non-cooperative game in which each firm aims at optimizing its own objective function.

By Lemma 2.1, firm i's optimal insurance purchase is uniquely determined, if both q_i and $\tilde{p}_i = \tilde{p}_i\left(q_{-i}\right)$ are given. Write $\hat{a}_i = \hat{a}_i\left(q_i, q_{-i}\right) = \hat{a}_i\left(q\right) \in [0, 1]$ to emphasize this relationship. From this, we can also infer that in the non-cooperative game, each firm essentially only has one decision variable, its investment in cybersecurity. Therefore, the game is characterized by each firm i aiming to optimize $\hat{u}_i\left(q_i, q_{-i}\right)$, defined below, via a choice of $q_i \in [0, 1]$:

$$\hat{u}_i\left(q_i, q_{-i}\right) = (1-q_i)\,\tilde{p}_i\mathbb{E}\left[U_i\left(W_i - (1-\hat{a}_i)L_i\right)\right] + \left(1-(1-q_i)\,\tilde{p}_i\right)\mathbb{E}\left[U_i\left(W_i\right)\right] - c_i\left(q_i\right) - \hat{a}_i\pi_i. \quad (4.1)$$

Based on (4.1), we present a formal definition of the pure-strategy Nash equilibrium of cybersecurity investments and insurance purchases.

Definition 4.1 *A vector $q^N \in [0, 1]^d$ of cybersecurity levels is a pure-strategy Nash equilibrium if it holds for all $i \in \{1, \ldots, d\}$ that*

$$\hat{u}_i\left(q_i^N, q_{-i}^N\right) \geq \hat{u}_i\left(q_i, q_{-i}^N\right), \quad \textit{for all } q_i \in [0, 1].$$

The corresponding vector a^N of equilibrium insurance coverage ratios is given by:

$$a^N = \left(\hat{a}_1\left(q^N\right), \ldots, \hat{a}_d\left(q^N\right)\right),$$

where each $\hat{a}_i$ is a firm-specific version of the function introduced in (2.4).

Roughly speaking, a Nash equilibrium is achieved when no firm can unilaterally improve its objective function by deviating from its current decisions. The following result presents the set of equations that a Nash equilibrium must satisfy.

Theorem 4.1 *(Characterization of Nash equilibrium). If for all $i \in \{1, \ldots, d\}$, the following boundary conditions hold*

$$c_i'\left(0\right) = 0 \quad \textit{and} \quad \lim_{q\to 1} c_i'\left(q\right) = \infty, \quad (4.2)$$

and that $\hat{u}_i\left(q_i, q_{-i}\right)$ is concave in $q_i \in [0, 1]$, then q^N is a pure-strategy Nash equilibrium as in Definition 4.1 if and only if it solves the following system of equations:

$$c_i'\left(q_i^N\right) = \tilde{p}_i\left(q_{-i}^N\right)\left(\mathbb{E}\left[U_i\left(W_i\right)\right] - \mathbb{E}\left[U_i\left(W_i - \left(1-\hat{a}_i\left(q^N\right)\right)L_i\right)\right]\right), \quad \textit{for } i \in \{1, \ldots, d\}. \quad (4.3)$$

Note that the strategy space of each firm is compact and, according to Lemma 2.2, the objective functions are concave under suitable conditions. The existence of a pure-strategy Nash equilibrium then follows directly from classical results in game theory; see, for example, Theorem 1 of Rosen (1965). For this reason, we omit a formal proof for the following theorem.

Theorem 4.2 *(Existence of Nash equilibrium). A pure-strategy Nash equilibrium as in Definition 4.1 exists, if for all $i \in \{1, \ldots, d\}$, the following inequality holds:*

$$c_i''\left(q\right) > \frac{\pi_i}{R_i}\frac{1}{\left(1-q\right)^2}, \quad \textit{for } q \in [0, 1), \quad (4.4)$$

where R_i is a coefficient defined as:

$$R_i = \inf_{a\in[0,1]} \frac{\mathbb{E}\left[-U_i''\left(W_i - (1-a)L_i\right)L_i^2\right]}{\mathbb{E}\left[U_i'\left(W_i - (1-a)L_i\right)L_i\right]}, \quad (4.5)$$

which is a firm-specific version of the coefficient introduced in (2.9).

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

The existence of Nash equilibrium does not guarantee uniqueness, as illustrated by the well-known example of the Battle of the Sexes, also known as Bach or Stravinsky; see Example 15.3 of Osborne and Rubinstein (1994). It is straightforward to establish that a symmetric equilibrium, where all firms make the same decisions, exists and is unique under the strict concavity condition in (4.4). However, this does not imply that non-symmetric equilibria do not exist.

A slightly stronger condition than (4.4) ensures the uniqueness of equilibrium under certain homogeneity conditions regarding objective functions, as shown in the following theorem.

Theorem 4.3 *(Uniqueness of Nash equilibrium under homogeneity conditions). Assume that $(c_i, \pi_i, U_i, W_i, L_i)$ for $i \in \{1, \ldots, d\}$ are copies of (c, π, U, W, L). If the following inequality holds:*

$$c''(q) \geq \frac{\pi}{R} \frac{1}{(1-q)^2} + \mathbb{E}\left[U'(W-L)L\right] \max\left\{1, \frac{1}{R}\right\}, \quad \text{for } q \in [0, 1), \tag{4.6}$$

where R is introduced in (2.9), then a pure-strategy Nash equilibrium as in Definition 4.1 exists and is unique.

If homogeneity does not hold, a condition stronger than (4.6) is required to establish the uniqueness of Nash equilibrium. The following uniqueness result for general setups builds upon Rosen's (1965) proof of equilibrium uniqueness based on diagonal strict concavity. The result implies that, if the convexity of each c_i is large enough, then there exists a unique pure-strategy Nash equilibrium.

Theorem 4.4 *(Uniqueness of Nash equilibrium). If for all $i \in \{1, \ldots, d\}$, the following inequality holds:*

$$\begin{aligned} c_i''(q) \geq{}& \frac{\pi_i}{R_i} \frac{1}{(1-q)^2} + \frac{d-1}{2} E\left[U_i'(W_i - L_i) L_i\right] \max\left\{1, \frac{1}{R_i}\right\} \\ &+ \frac{1}{2} \sum_{j=1, j\neq i}^{d} \mathbb{E}\left[U_j'\left(W_j - L_j\right) L_j\right] \max\left\{1, \frac{1}{R_j}\right\}, \quad \text{for } q \in [0, 1), \end{aligned} \tag{4.7}$$

where each R_i is defined in (4.5), then a pure-strategy Nash equilibrium as in Definition 4.1 exists and is unique.

Though seemingly strange, convexity conditions similar to (4.4), (4.6), and (4.7) are common in the study of Nash equilibrium. For example, Acemoglu *et al.* (2016) and Nagurney and Shukla (2017) impose similar convexity conditions on their cost functions to ensure the existence or uniqueness of Nash equilibrium. That said, these conditions are easily verifiable in numerical examples, which guarantees the feasibility of finding Nash equilibrium numerically.

We further provide Proposition 4.1 below as an extension of Proposition 2.1 under the network setup, which follows directly from (A8) in the proof of Theorem 4.3. It shows that a firm's optimal decision on its insurance coverage ratio decreases not only with its own cybersecurity level but also with those of the other firms in the network. Intuitively, the higher any firm's cybersecurity level, the lower the probability of a compromise, and thus, the less demand for insurance coverage.

Proposition 4.1 *(Monotonicity of insurance coverage ratios with cybersecurity levels). Recall that firm i's optimal insurance coverage ratio $\hat{a}_i = \hat{a}_i(q)$ is a function of all firms' cybersecurity levels. For any $i, j \in \{1, \ldots, d\}$, it holds that $\frac{\partial \hat{a}_i}{\partial q_j} \leq 0$.*

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

4.2 Inefficiency of the Nash equilibrium

It is well known that in Nash equilibria, firms only optimize their own objective functions, which may lead to inefficient outcomes for all firms as a collective (as in the well-known Prisoner's Dilemma). We now present two results regarding the inefficiency of the Nash equilibrium within our framework.

Proposition 4.2 *(Underinvestment compared to a social optimum). Define a social welfare function as the sum of the objective functions of all d firms in the network:*

$$\hat{u}_S(q) = \sum_{i=1}^{d} \hat{u}_i\left(q_i, q_{-i}\right).$$

Under the conditions of Theorem 4.3, for any symmetric network, there exists a unique symmetric Nash equilibrium with a uniform security level q^N, and a unique symmetric social optimum with a uniform security level q^S, satisfying $q^N \leq q^S$.

The first result above compares the Nash equilibrium to a social welfare optimum under homogeneity and symmetry conditions. It shows that firms underinvest in cybersecurity under the Nash equilibrium, which is less beneficial for all firms as a collective. As a result, firms purchase more insurance under the Nash equilibrium than under the social optimum due to the monotonicity of the optimal insurance coverage ratios in the cybersecurity levels established in Proposition 4.1. The following result demonstrates that the Nash equilibria is not Pareto efficient in more general settings.

Proposition 4.3 *(Pareto inefficiency). For any Nash equilibrium, if there exists a linkage between two firms whose insurance coverage ratios and cybersecurity levels under this equilibrium are all strictly less than 1, then this equilibrium is not Pareto efficient.*

The inefficiency of a Nash equilibrium can be understood as follows. In a Nash equilibrium, one offsets the cost of purchasing cybersecurity with the benefits from being protected itself. A firm does not consider the positive side effect of purchasing cybersecurity on other participants. A social planner like in Proposition 4.2, however, is able to balance the costs of one firm with the benefits on cybersecurity for the collective, which is more welfare improving.

5. Numerical studies

The existence and uniqueness results for the Nash equilibrium, as in Definition 4.1, allow us to numerically gain insights into firms' equilibrium decisions on cybersecurity investments and insurance purchases. In this section, we present three numerical studies with five firms and different network configurations. These considerations provide conveniences in terms of tractability without sacrificing any insights. We assume some homogeneity among the firms. In particular, for illustration purposes, we specify that

- Each firm has the same utility function (2.10) with a coefficient of absolute risk aversion of $\rho = 1$.
- Each firm generates a terminal revenue of $W = 1$, and once compromised, it loses all its revenue, that is, $L = 1$.
- The network structure, the cybersecurity cost function, and the insurance premium will vary from one example to another and will be specified in later subsections.

Referring back to Example 2.1, the above specifications result in $R = 1$.

5.1 A homogeneous complete network

The first network structure we consider is a complete network, where all nodes are connected to each other, as plotted in Figure 2. This type of network is arguably the most popular network structure, where

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

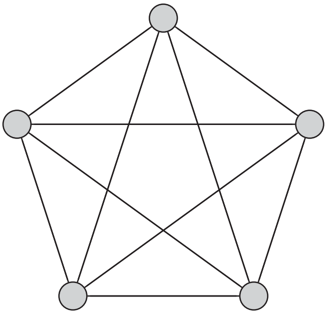

Figure 2. *This figure depicts a complete network of five firms, with each firm connected to all the others.*

information can be exchanged conveniently. A real-world example is that financial institutions perform trades with each other, allowing malware to spread from one to another through email attachments, media, etc.

In this subsection, we also assume that a uniform cost function $c(\cdot)$ and a uniform full-coverage premium π, which is less than or equal to the constant loss $L = 1$ at compromise, apply to all firms. Due to the homogeneity, by Theorem 4.3, a sufficient condition for the game to have a unique Nash equilibrium is

$$c''(q) > \frac{\pi}{R}\frac{1}{(1-q)^2} + \mathbb{E}\left[U'(W-L)L\right]\max\left\{1, \frac{1}{R}\right\} = \frac{\pi}{(1-q)^2} + 1, \quad \text{for } q \in [0, 1).$$

Clearly, the cost function

$$c(q) = -\ln(1-q) - q + \frac{2}{3}q^2 \tag{5.1}$$

satisfies the convexity condition.

Since the Nash equilibrium is unique under the cost function $c(\cdot)$ in (5.1), and the complete network is symmetric, the unique equilibrium must also be symmetric. Otherwise, multiple non-symmetric Nash equilibria would exist. Therefore, the equilibrium decision on the cybersecurity levels is characterized by a vector q^N with all elements identical to some constant, q^N. Then the equilibrium decisions on the insurance coverage ratios are subsequently determined and must also be the same.

Now that we know the cybersecurity levels are identical in the equilibrium, for the complete network of five firms, it is easy to see that the probability of infection reaching a firm is given by:

$$\tilde{p}_i\left(q^N\right) = \frac{1}{5} + \frac{4}{5}\left(1 - q^N\right).$$

Substituting this into (4.1) leads to an objective function that can be easily optimized numerically. Table 1 summarizes the numerical values of the identical insurance coverage ratio, a^N, and the identical cybersecurity level, q^N, in the unique equilibrium under different values of the full-coverage premium, π. These results indicate that when premiums are lower, firms tend to purchase more insurance and reduce investment in cybersecurity. Conversely, as cybersecurity investment increases, the allocation to insurance coverage decreases, which is consistent with Propositions 2.1, 2.2, and 4.1.

5.2 Homogeneous networks of arbitrary structure

While complete networks have their advantages in terms of popularity and explicitness, it is often the case that the exact structure of firm connections is unclear. Therefore, we next consider general network structures in which firms may or may not be linked together.

Similar to the previous subsection, we assume a uniform cost function, $c(\cdot)$, and a uniform full-coverage premium, π, that apply to all firms. Same as before, Theorem 4.3 is applicable, and hence,

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

Table 1. *Considering a complete network under homogeneity conditions, there exists a unique symmetric Nash equilibrium for the cost function $c(\cdot)$ in (5.1). This table summarizes the equilibrium decisions across different values of the full-coverage premium.*

Full-coverage premium π	0.3	0.4	0.5	0.6
Equilibrium insurance coverage ratio a^N	1	0.820	0.213	0
Equilibrium cybersecurity level q^N	0	0.0521	0.237	0.301

Table 2. *Considering networks of arbitrary structure under homogeneity conditions, there exists a unique Nash equilibrium for the cost function $c(\cdot)$ in (5.1). This table summarizes the equilibrium decisions of firms having the same number of connections, averaged over all network structures and across different values of full-coverage premiums, along with additional data.*

	$\pi = 0.3$		$\pi = 0.4$		$\pi = 0.5$		$\pi = 0.6$	
Degree	a^N	q^N	a^N	q^N	a^N	q^N	a^N	q^N
0	0	0.0529	0	0.0529	0	0.0529	0	0.0529
1	0.854	0.0141	0.629	0.0477	0.291	0.107	0.0291	0.1580
2	0.972	0.00320	0.780	0.0327	0.430	0.0961	0.1343	0.1578
3	0.997	0.000395	0.841	0.0250	0.488	0.0901	0.1635	0.1593
4	1	0	0.881	0.0194	0.537	0.0833	0.2129	0.1535

under the cost function specified in (5.1), the Nash equilibrium exists and is unique. We then explore all possible networks of five firms, resulting in a total of $2^{\binom{5}{2}} = 1,024$ possibilities. Among these possibilities, each firm has 0 connections in 64 cases, 1 connection in 256 cases, 2 connections in 384 cases, 3 connections in 256 cases, and 4 connections in 64 cases. In short, the setup here can be viewed as an extension of the previous example. The difference is that the network structure is not restricted to a complete network, while everything else remains unchanged.

For a given, uniform full-coverage premium π, we use a recursive numerical algorithm to calculate the equilibrium decisions for each firm. In this recursive algorithm, at each step, each firm optimizes its own objective function by considering the decisions of the other firms from the previous step. The process continues until the values of the decision variables converge. The results of equilibrium are then grouped and averaged based on the number of connections a firm has, as presented in Table 2. From this table, we observe that isolated firms do not purchase any insurance at all for the four considered values of π. This is because these considered values all exceed 0.2, which is the expected loss for a firm with no connection. We also notice that as premiums become more expensive, firms tend to invest more in cybersecurity and purchase less insurance, consistent with the previous numerical example. Additionally, firms with more connections, which are more likely to be reached by the infection during a cyber incident, generally purchase more insurance and invest less in protection.

If the number of firms d increases, solving the equilibrium for all possible networks becomes exponentially complex, since there are $2^{\binom{d}{2}}$ possible network configurations. A tractable solution is to generate a smaller set of random networks, which have probabilistic contagion links. For a further discussion on random networks, we refer to Acemoglu *et al*. (2016).

5.3 An example with differentiated insurance premiums

The insurance premium in the previous two subsections has been setup in an *ad hoc* manner. It applies uniformly to all firms, regardless of their network connections. However, firms with more connections may face a higher risk of exposure and, consequently, could potentially be subject to a higher premium.

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

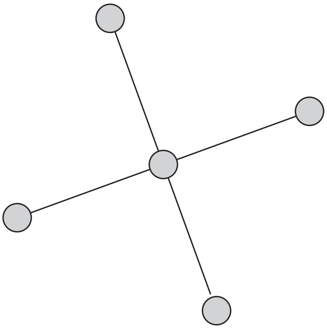

__Figure 3.__ This figure depicts a star network of five firms, including a central firm and four peripheral firms.

Therefore, it is also interesting to differentiate the premiums across firms and examine the equilibrium decisions. Since the premiums may now differ among firms, violating the homogeneity condition in Theorem 4.3, we apply the more general Theorem 4.4 instead. We adopt a cost function that satisfies the condition in (4.7) and is more convex than the one in (5.1) to ensure the existence of a unique Nash equilibrium. More specifically, we consider the same cost function for the central and peripheral firms, as follows:

$$c\left(q\right)=-\ln\left(1-q\right)-q+\frac{5}{2}q^{2}. \tag{5.2}$$

We focus on a specific network type, a star network, which offers two main advantages. First, it allows for heterogeneity between the central and peripheral nodes while maintaining homogeneity among the peripheral nodes. Second, it is analytically tractable, allowing us to derive explicit expressions for the compromise probabilities of the firms, as explained in more detail below. In real-world context, there are numerous examples of star networks. For instance, businesses rely on cloud-based services such as Amazon Web Services, and financial institutions often process transactions through third-party clearinghouses.

A star network consisting of five firms includes a central firm and four peripheral firms, as plotted in Figure 3. We continue to consider the same utility function, terminal revenue, and potential cyber loss for all firms, as mentioned at the beginning of this section. Since the peripheral firms are symmetric to each other in terms of network positions, it is reasonable to assume that they are each charged the same full-coverage insurance premium. We use subscript 1 to indicate the central firm and subscript 2 to indicate the peripheral firms. For example, π_1 and π_2 represent the full-coverage insurance premiums for the central and peripheral firms, respectively.

Similar to the discussions in the Subsection 5.1 for a complete network, the peripheral firms must make identical decisions in the unique equilibrium. Otherwise, multiple non-symmetric Nash equilibria would exist. Consequently, the equilibrium decisions on the insurance coverage ratios are also identical across the peripheral firms.

Denote by $\left(a_1^N, q_1^N\right)$ and $\left(a_2^N, q_2^N\right)$ the equilibrium decisions of the central firm and the peripheral firms, respectively. Then the probability of infection reaching the central firm can be easily derived as:

$$\tilde{p}_1\left(q_2^N\right)=\frac{1}{5}+\frac{4}{5}\left(1-q_2^N\right),$$

and the probability of infection reaching the peripheral firms is given by:

$$\tilde{p}_2\left(q_1^N, q_2^N\right)=\frac{1}{5}+\frac{1}{5}\left(1-q_1^N\right)+\frac{3}{5}\left(1-q_1^N\right)\left(1-q_2^N\right).$$

Note that $\tilde{p}_2$ depending on q_2^N is not a mistake but rather occurs because multiple peripheral firms make the same equilibrium decision regarding the cybersecurity level.

Table 3. *Consider a star network where homogeneity conditions are assumed for the peripheral firms, while the premiums and cost functions differ across the central firm and the peripheral firms. There exists a unique Nash equilibrium in which the peripheral firms make identical equilibrium decisions for the cost function $c(\cdot)$ in (5.2). This table summarizes the equilibrium decisions across different values of full-coverage premiums, with subscript 1 indicating the central firm and subscript 2 indicating the peripheral firms.*

Full-coverage premiums (π_1, π_2)	$(0.5, 0.5)$	$(0.8, 0.5)$	$(0.8, 0.6)$
Equilibrium insurance coverage ratios $\left(a_1^N, a_2^N\right)$	$(0.663, 0.885)$	$(0.111, 0.576)$	$(0.0934, 0.360)$
Equilibrium cybersecurity levels $\left(q_1^N, q_2^N\right)$	$(0.0244, 0.00731)$	$(0.0845, 0.0296)$	$(0.0856, 0.0493)$

By applying a recursive numerical algorithm, we obtain the Nash equilibrium strategies for different values of π_1 and π_2, and we summarize the results in Table 3. The results suggest that the lower the full-coverage premiums, the higher the insurance coverage that firms seek, and the less they invest in cybersecurity. This leads to an increase in the risk borne by the insurer, potentially leading to significant losses for the insurer. Conversely, charging higher premiums would result in a contraction of the market for insurers. In particular, as the premium for the central firm, π_1, increases, it purchases less insurance but invests more in cybersecurity. Interestingly, the peripheral firms also invest more in cybersecurity in response. Due to increased cybersecurity levels across all firms, the optimal insurance coverage ratios are reduced, as implied by Proposition 4.1. These results are consistent with our expectations: Firms tend to invest little in cybersecurity protection due to the convexity of the cost function, which means that the provision of insurance is costly.

6. Concluding remarks

In this paper, we investigate a network of interconnected firms and analyze their cybersecurity investments and insurance purchases. We employ the random attack model proposed by Acemoglu *et al.* (2016), in which a cyber incident begins when an attacker randomly targets a firm and ends when no further firms are compromised in a cascade of compromises starting from the targeted firm. The probability of a firm being eventually compromised relies on its individual cybersecurity level and the cybersecurity levels of other network members. Firms can choose to invest in cybersecurity practices to reduce the probability of being breached and to purchase cyber insurance to receive *ex post* reimbursement if a cyber loss occurs. We show that, for a given cybersecurity level, the optimal insurance coverage ratio is uniquely determined, thus simplifying the decision-making process from a bivariate to a univariate decision game. We also find that cybersecurity investments and insurance purchases act as strategic complements: increased insurance coverage leads to reduced investment in cybersecurity, and vice versa, increased investment in cybersecurity leads to reduced insurance coverage. We then establish the existence and uniqueness of the Nash equilibrium and present two results demonstrating its inefficiency. Finally, we conduct extensive numerical studies to examine firms' equilibrium decisions under various network structures and explore the interplay between the two decision variables.

We conclude this paper with two future research directions. First, in our current study, the insurer sets the price and does not adjust it based on the firms' decisions, which can alter their risk profile. Exploring a two-stage game in which the insurer actively optimizes its expected profit by anticipating firms' responses would be an interesting avenue. Second, in practice, cyber criminals might be more incentivized to target firms with insurance protection and lower security levels. Considering strategic criminals who tend to target more vulnerable firms would be an interesting direction for future research.

Acknowledgment. The authors thank the referees for their thoughtful and constructive comments, which bring valuable insights toward improving the manuscript. Zhiwei Tong appreciates the generous startup fund provided by the Department of Statistics and Actuarial Science and the Old Gold Summer Fellowship provided by the College of Liberal Arts and Sciences, both at the University of Iowa. Yang Feng appreciates the TP-A1 startup research grant provided by the University of Science and Technology Beijing.

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

References

Acemoglu, D., Malekian, A. and Ozdaglar, A. (2016) Network security and contagion. *Journal of Economic Theory*, **166**, 536–585.

Agrafiotis, I., Nurse, J.R., Goldsmith, M., Creese, S. and Upton, D. (2018) A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, **4**(1), 1–15.

Albrecher, H., Beirlant, J. and Teugels, J.L. (2017) Reinsurance: Actuarial and Statistical Aspects. Hoboken, New Jersey: John Wiley and Sons.

Awiszus, K., Bell, Y., Lüttringhaus, J., Svindland, G., Voß, A. and Weber, S. (2024) Building resilience in cybersecurity: An artificial lab approach. *Journal of Risk and Insurance*, **91**(3), 753–800.

Awiszus, K., Knispel, T., Penner, I., Svindland, G., Voß, A. and Weber, S. (2023) Modeling and pricing cyber insurance: Idiosyncratic, systematic, and systemic risks. *European Actuarial Journal*, **13**(1), 1–53.

Biener, C., Eling, M. and Wirfs, J.H. (2015) Insurability of cyber risk: An empirical analysis. *Geneva Papers on Risk and Insurance - Issues and Practice*, **40**, 131–158.

Boonen, T.J. and Liu, F. (2022) Insurance with heterogeneous preferences. *Journal of Mathematical Economics*, **102**, 102742.

Braun, A., Eling, M. and Jaenicke, C. (2023) Cyber insurance-linked securities. *ASTIN Bulletin: The Journal of the IAA*, **53**(3), 684–705.

Da, G., Xu, M. and Zhao, P. (2021) Multivariate dependence among cyber risks based on L-hop propagation. *Insurance: Mathematics and Economics*, **101**, 525–546.

Dacorogna, M. and Kratz, M. (2023) Managing cyber risk, a science in the making. *Scandinavian Actuarial Journal*, **2023**, 1–22.

Eisenbach, T.M., Kovner, A. and Lee, M.J. (2022) Cyber risk and the US financial system: A pre-mortem analysis. *Journal of Financial Economics*, **145**(3), 802–826.

Eling, M. (2020) Cyber risk research in business and actuarial science. *European Actuarial Journal*, **10**(2), 303–333.

Eling, M., McShane, M. and Nguyen, T. (2021) Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, **24**(1), 93–125.

Fahrenwaldt, M.A., Weber, S. and Weske, K. (2018) Pricing of cyber insurance contracts in a network model. *ASTIN Bulletin: The Journal of the IAA*, **48**(3), 1175–1218.

Hillairet, C., Lopez, O., d'Oultremont, L. and Spoorenberg, B. (2022) Cyber-contagion model with network structure applied to insurance. *Insurance: Mathematics and Economics*, **107**, 88–101.

Jevtić, P. and Lanchier, N. (2020) Dynamic structural percolation model of loss distribution for cyber risk of small and medium-sized enterprises for tree-based LAN topology. *Insurance: Mathematics and Economics*, **91**, 209–223.

Khalili, M.M., Naghizadeh, P. and Liu, M. (2017) Designing cyber insurance policies: Mitigating moral hazard through security pre-screening. *GAMENETS*, pp. 63–73. Springer International Publishing.

Marotta, A., Martinelli, F., Nanni, S., Orlando, A. and Yautsiukhin, A. (2017) Cyber-insurance survey. *Computer Science Review*, **24**, 35–61.

Mott, G., Turner, S., Nurse, J.R., MacColl, J., Sullivan, J., Cartwright, A. and Cartwright, E. (2023) Between a rock and a hard(ening) place: Cyber insurance in the ransomware era. *Computers and Security*, **128**, 103162.

Nagurney, A. and Shukla, S. (2017) Multifirm models of cybersecurity investment competition vs. cooperation and network vulnerability. *European Journal of Operational Research*, **260**(2), 588–600.

Ogut, H., Menon, N. and Raghunathan, S. (2005) Cyber insurance and it security investment: Impact of interdependence risk. Available at https://infosecon.net/workshop/pdf/56.pdf.

Osborne, M.J. and Rubinstein, A. (1994) *A Course in Game Theory*. Cambridge, Massuchusetts, USA: MIT Press.

Pal, R. (2012) *Cyber-insurance in internet security: A dig into the information asymmetry problem*. Preprint. Available at https://arxiv.org/abs/1202.0884.

Pal, R., Golubchik, L., Psounis, K. and Hui, P. (2014) Will cyber-insurance improve network security? A market analysis. *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*, pp. 235–243.

Pal, R., Golubchik, L., Psounis, K. and Hui, P. (2019) Security pricing as enabler of cyber-insurance a first look at differentiated pricing markets. *IEEE Transactions on Dependable and Secure Computing*, **16**(2), 358–372.

Peng, C., Xu, M., Xu, S. and Hu, T. (2018) Modeling multivariate cybersecurity risks. *Journal of Applied Statistics*, **45**(15), 2718–2740.

Rosen, J.B. (1965) Existence and uniqueness of equilibrium points for concave N-person games. *Econometrica*, **33**(3), 520–534.

Schwartz, G.A. and Sastry, S.S. (2014) Cyber-insurance framework for large scale interdependent networks. *Proceedings of the 3rd International Conference on High Confidence Networked Systems*, pp. 145–154.

Shetty, N., Schwartz, G., Felegyhazi, M. and Walrand, J. (2010) Competitive cyber-insurance and internet security. In *Economics of Information Security and Privacy* (eds. T. Moore, D. Pym and C. Ioannidis), pp. 229–247. New York: Springer, USA.

Xiang, Q., Neufeld, A., Peters, G.W., Nevat, I. and Datta, A. (2024) A bonus-malus framework for cyber risk insurance and optimal cybersecurity provisioning. *European Actuarial Journal*, **14**(2), 581–621.

Xu, M. and Hua, L. (2019) Cybersecurity insurance: Modeling and pricing. *North American Actuarial Journal*, **23**(2), 220–249.

Yang, Z. and Lui, J.C. (2014) Security adoption and influence of cyber-insurance markets in heterogeneous networks. *Performance Evaluation*, **74**, 1–17.

Zeller, G. and Scherer, M. (2023) Risk mitigation services in cyber insurance: Optimal contract design and price structure. *Geneva Papers on Risk and Insurance - Issues and Practice*, **48**, 502–547.

Zhang, X., Xu, M., Su, J. and Zhao, P. (2023) Structural models for fog computing based internet of things architectures with insurance and risk management applications. *European Journal of Operational Research*, **305**(3), 1273–1291.

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

Appendix

Proof of Lemma 2.1

Taking the first and second partial derivatives of $u\,(a, q)$ with respect to a yields

$$\frac{\partial u}{\partial a} = \mathbb{E}\left[U'\,(W-(1-a)LY)\,(LY)\right] - \pi \tag{A1}$$

and

$$\frac{\partial^2 u}{\partial a^2} = \mathbb{E}\left[U''\,(W-(1-a)LY)\,(LY)^2\right]. \tag{A2}$$

Recalling that $P\,(Y=1) = p = (1-q)\,\tilde{p}$, it is easy to see that the first-order condition $\frac{\partial u}{\partial a} = 0$ is equivalent to (2.5).

When $q = 1$, that is, the firm is fully immune against cyberattacks, the compromise indicator Y degenerates at 0, and hence $\frac{\partial u}{\partial a} < 0$. This shows that $u\,(a, 1)$ is strictly decreasing in a, and the unique $a \in [0, 1]$ that maximizes $u\,(a, 1)$ is $a = 0$. When $q < 1$, it holds that $P\,(Y=1) = p = (1-q)\,\tilde{p} > 0$, and hence $\frac{\partial^2 u}{\partial a^2} < 0$. This shows that $u\,(a, q)$, given a fixed $q \in [0, 1)$, is strictly concave over $a \in [0, 1]$, thereby ensuring the uniqueness of the maximizer. In summary, for any given $q \in [0, 1]$, there exists a unique maximizer of $u\,(a, q)$.

Now let us consider the first derivative $\frac{\partial u}{\partial a}$ at the boundaries. At $a = 0$, by (A1),

$$\left.\frac{\partial u}{\partial a}\right|_{a=0} = \mathbb{E}\left[U'\,(W-LY)\,(LY)\right] - \pi = (1-q)\,\tilde{p}\mathbb{E}\left[U'\,(W-L)\,L\right] - \pi,$$

which satisfies $\left.\frac{\partial u}{\partial a}\right|_{a=0} \le 0$ if and only if

$$q \ge 1 - \frac{\pi}{\tilde{p}\mathbb{E}\,[U'\,(W-L)\,L]}.$$

At $a = 1$, again by (A1),

$$\left.\frac{\partial u}{\partial a}\right|_{a=1} = \mathbb{E}\left[U'\,(W)\,(LY)\right] - \pi = (1-q)\,\tilde{p}\mathbb{E}\left[U'\,(W)\,L\right] - \pi,$$

which satisfies $\left.\frac{\partial u}{\partial a}\right|_{a=1} \ge 0$ if and only if

$$q \le 1 - \frac{\pi}{\tilde{p}\mathbb{E}\,[U'\,(W)\,L]}.$$

Basing on the above discussions, and recalling the concavity of $u\,(a, q)$ in a, we conclude:

Case 1: $\pi \ge \tilde{p}\mathbb{E}\,[U'\,(W-L)\,L]$. *For any* $q \in [0, 1]$, *it holds that* $\left.\frac{\partial u}{\partial a}\right|_{a=0} \le 0$, *showing* $\hat{a}(q) = 0$.

Case 2: $\tilde{p}\mathbb{E}\,[U'\,(W)\,L] < \pi < \tilde{p}\mathbb{E}\,[U'\,(W-L)\,L]$. *For any* $q \in [0, 1]$, *it holds that* $\left.\frac{\partial u}{\partial a}\right|_{a=1} < 0$, *showing* $\hat{a}(q) < 1$. *For* $q \in \left[0, 1 - \frac{\pi}{\tilde{p}\mathbb{E}\left[U'(W-L)L\right]}\right)$, *it holds that* $\left.\frac{\partial u}{\partial a}\right|_{a=0} > 0$, *showing that* $\hat{a}(q)$ *solves (2.5). For* $q \in \left[1 - \frac{\pi}{\tilde{p}\mathbb{E}\left[U'(W-L)L\right]}, 1\right]$, *it holds that* $\left.\frac{\partial u}{\partial a}\right|_{a=0} \le 0$, *showing* $\hat{a}(q) = 0$.

Case 3: $\pi \le \tilde{p}\mathbb{E}\,[U'\,(W)\,L]$. *For* $q \in \left[0, 1 - \frac{\pi}{\tilde{p}\mathbb{E}\left[U'(W)L\right]}\right]$, *it holds that* $\left.\frac{\partial u}{\partial a}\right|_{a=1} \ge 0$, *showing* $\hat{a}(q) = 1$. *For* $q \in \left(1 - \frac{\pi}{\tilde{p}\mathbb{E}\left[U'(W)L\right]}, 1 - \frac{\pi}{\tilde{p}\mathbb{E}\left[U'(W-L)L\right]}\right)$, *it holds that* $\left.\frac{\partial u}{\partial a}\right|_{a=0} > 0$ *and* $\left.\frac{\partial u}{\partial a}\right|_{a=1} < 0$, *showing* $\hat{a}(q)$ *solves (2.5). For* $q \in \left[1 - \frac{\pi}{\tilde{p}\mathbb{E}\left[U'(W-L)L\right]}, 1\right]$, *it holds that* $\left.\frac{\partial u}{\partial a}\right|_{a=0} \le 0$, *showing* $\hat{a}(q) = 0$.

Proof of Lemma 2.2

By Lemma 2.1, we know that $\hat{a}\,(q)$ can be a piecewise function over different subintervals of [0, 1]. Nevertheless, it either satisfies the first-order condition (2.5) or is constant at 0 or 1. Therefore, for q in

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

the interior of the subintervals, either $\frac{\partial u}{\partial a}\left(\hat{a}\left(q\right),q\right)=0$ or $\hat{a}'\left(q\right)=0$. Thus, the first derivative of $\hat{u}\left(q\right)$ at any interior point of the subintervals is given by:

$$\begin{aligned}\hat{u}'\left(q\right)&=\frac{\partial u}{\partial a}\left(\hat{a}\left(q\right),q\right)\hat{a}'\left(q\right)+\frac{\partial u}{\partial q}\left(\hat{a}\left(q\right),q\right)=\frac{\partial u}{\partial q}\left(\hat{a}\left(q\right),q\right)\\&=-\tilde{p}\mathbb{E}\left[U\left(W-\left(1-\hat{a}\left(q\right)\right)L\right)\right]+\tilde{p}\mathbb{E}\left[U\left(W\right)\right]-c'\left(q\right),\end{aligned}\tag{A3}$$

and consequently, the second derivative is given by:

$$\hat{u}''\left(q\right)=-\tilde{p}\mathbb{E}\left[U'\left(W-\left(1-\hat{a}\left(q\right)\right)L\right)L\right]\hat{a}'\left(q\right)-c''\left(q\right).\tag{A4}$$

If q is an interior point of a subinterval corresponding to $\hat{a}\left(q\right)=0$ or 1, then $\hat{a}'\left(q\right)=0$, and hence, $\hat{u}''\left(q\right)=-c''\left(q\right)<0$.

If q is an interior point of a subinterval corresponding to $\hat{a}\left(q\right)=\tilde{a}\left(q\right)$, then by (2.5) and the condition in (2.8),

$$\hat{u}''\left(q\right)=-\pi\frac{\tilde{a}'\left(q\right)}{1-q}-c''\left(q\right).\tag{A5}$$

For the first term on the right-hand side of (A5), recall (2.6) and write

$$-\pi\frac{\tilde{a}'\left(q\right)}{1-q}=\pi\frac{\mathbb{E}\left[U'\left(W-\left(1-\tilde{a}\left(q\right)\right)L\right)L\right]}{\left(1-q\right)^{2}\mathbb{E}\left[-U''\left(W-\left(1-\tilde{a}\left(q\right)\right)L\right)L^{2}\right]}\leq\frac{\pi}{R}\frac{1}{\left(1-q\right)^{2}},\tag{A6}$$

showing that in this case $\hat{u}''\left(q\right)<0$ under the condition in (2.8).

The above analysis shows that $\hat{u}\left(q\right)$ is concave over each of the subintervals of [0, 1]. We further claim that it is concave over [0, 1]. This can be seen from the fact that both $\hat{u}\left(q\right)$ and $\hat{u}'\left(q\right)$ are continuous in $\hat{a}\left(q\right)$, as shown by (A3), and the fact that $\hat{a}\left(q\right)$ itself is continuous in $q\in[0,1]$, as concluded in Proposition 2.1.

Proof of Theorem 4.1

By Definition 4.1, the equilibrium cybersecurity levels, q_i^N, for $i\in\{1,\ldots,d\}$, must satisfy

$$q_i^N\in\arg\max_{q_i\in[0,1]}\hat{u}_i\left(q_i,q_{-i}^N\right).$$

Recalling (A3), the first partial derivative of $\hat{u}_i\left(q_i,q_{-i}\right)$ with respect to q_i is given by:

$$\frac{\partial\hat{u}_i}{\partial q_i}=-\tilde{p}_i\mathbb{E}\left[U_i\left(W_i-(1-\hat{a}_i)L_i\right)\right]+\tilde{p}_i\mathbb{E}\left[U_i\left(W_i\right)\right]-c_i'\left(q_i\right).$$

It is easy to see that under the boundary conditions in (4.2),

$$\left.\frac{\partial\hat{u}_i}{\partial q_i}\right|_{q_i=0}\geq 0\quad\text{and}\quad\left.\frac{\partial\hat{u}_i}{\partial q_i}\right|_{q_i\to 1}=-\infty.$$

By the concavity of $\hat{u}_i\left(q_i,q_{-i}\right)$ in q_i, as the maximizer of $\hat{u}_i$, q_i^N must satisfy $\left.\frac{\partial\hat{u}_i}{\partial q_i}\right|_{q_i=q_i^N}=0$ and hence leads to (4.3).

Proof of Theorem 4.3

Considering the objective functions $\hat{u}_i\left(q_i,q_{-i}\right)$ in (4.1), according to Rosen (1965), a condition for the game to have a unique pure-strategy Nash equilibrium is that $\left(\hat{u}_1,\ldots,\hat{u}_d\right)$ is diagonally strictly concave. Rosen (1965) also shows that a sufficient condition is that $J+J^{\intercal}$, where J is a $d\times d$ matrix with (i,j)th element being $\frac{\partial^2\hat{u}_i}{\partial q_i\partial q_j}$, is negative definite over the strategy space $q\in[0,1]^d$. Our goal in this proof is to show that this holds.

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

We first derive a lower bound for the absolute value of the cross derivatives. Recalling (A3), the first partial derivative of $\hat{u}_i\left(q_i, q_{-i}\right)$ with respect to q_i is given by:

$$\frac{\partial \hat{u}_i}{\partial q_i} = -\tilde{p}_i \mathbb{E}\left[U_i\left(W_i - (1-\hat{a}_i)L_i\right)\right] + \tilde{p}_i \mathbb{E}\left[U_i\left(W_i\right)\right] - c_i'\left(q_i\right).$$

Further taking the partial derivative with respect to q_j yields

$$\frac{\partial^2 \hat{u}_i}{\partial q_i \partial q_j} = Q_{ij}\left(\mathbb{E}\left[U_i\left(W_i - (1-\hat{a}_i)L_i\right)\right] - \mathbb{E}\left[U_i\left(W_i\right)\right]\right) - \mathbb{E}\left[U_i'\left(W_i - (1-\hat{a}_i)L_i\right)L_i\right]\tilde{p}_i \frac{\partial \hat{a}_i}{\partial q_j}. \tag{A7}$$

By Lemma 2.1, we have either $\frac{\partial \hat{a}_i}{\partial q_j} = 0$ or

$$\left(1-q_i\right)\tilde{p}_i \mathbb{E}\left[U_i'\left(W_i - (1-\hat{a}_i)L_i\right)L_i\right] = \pi_i.$$

Taking the partial derivative with respect to q_j in the above equation yields

$$Q_{ij}\mathbb{E}\left[U_i'\left(W_i - (1-\hat{a}_i)L_i\right)L_i\right] = \mathbb{E}\left[U_i''\left(W_i - (1-\hat{a}_i)L_i\right)L_i^2\right]\tilde{p}_i \frac{\partial \hat{a}_i}{\partial q_j}.$$

Thus,

$$0 \geq \tilde{p}_i \frac{\partial \hat{a}_i}{\partial q_j} \geq -Q_{ij}\frac{\mathbb{E}\left[U_i'\left(W_i - (1-\hat{a}_i)L_i\right)L_i\right]}{\mathbb{E}\left[-U_i''\left(W_i - (1-\hat{a}_i)L_i\right)L_i^2\right]}. \tag{A8}$$

By the monotonicity of U_i,

$$\mathbb{E}\left[U_i\left(W_i - (1-\hat{a}_i)L_i\right)\right] - \mathbb{E}\left[U_i\left(W_i\right)\right] < 0, \tag{A9}$$

and by the concavity of U_i,

$$\begin{aligned}
&\left|\mathbb{E}\left[U_i\left(W_i - (1-\hat{a}_i)L_i\right)\right] - \mathbb{E}\left[U_i\left(W_i\right)\right]\right| \\
&\leq \mathbb{E}\left[U_i'\left(W_i - (1-\hat{a}_i)L_i\right)(1-\hat{a}_i)L_i\right] \\
&\leq \mathbb{E}\left[U_i'\left(W_i - (1-\hat{a}_i)L_i\right)L_i\right].
\end{aligned} \tag{A10}$$

Putting (A7)–(A10) together yields

$$\left|\frac{\partial^2 \hat{u}_i}{\partial q_i \partial q_j}\right| \leq \mathbb{E}\left[U_i'\left(W_i - (1-\hat{a}_i)L_i\right)L_i\right]\max\left\{1, \frac{\mathbb{E}\left[U_i'\left(W_i - (1-\hat{a}_i)L_i\right)L_i\right]}{\mathbb{E}\left[-U_i''\left(W_i - (1-\hat{a}_i)L_i\right)L_i^2\right]}\right\}.$$

Recalling the coefficient R_i introduced in (4.5), the inequality above can be rewritten as:

$$\left|\frac{\partial^2 \hat{u}_i}{\partial q_i \partial q_j}\right| \leq \mathbb{E}\left[U_i'\left(W_i - L_i\right)L_i\right]\max\left\{1, \frac{1}{R_i}\right\}. \tag{A11}$$

Now, let us recall equality (A5) and inequality (A6), which are about the second derivative of $\hat{u}_i\left(q_i, q_{-i}\right)$ with respect to q_i obtained in the setup of a single firm's decision problem. Using these results, we can derive

$$\left|\frac{\partial^2 \hat{u}_i}{\partial q_i^2}\right| \geq c_i''\left(q_i\right) + \frac{\pi}{1-q_i}\frac{\partial \tilde{a}_i}{\partial q_i} \geq c_i''\left(q_i\right) - \frac{\pi_i}{R_i}\frac{1}{\left(1-q_i\right)^2}. \tag{A12}$$

According to the homogeneity condition, the matrix $J + J^\intercal$ has identical diagonal elements and identical off-diagonal elements. Therefore, it is negative definite if the diagonal elements are negative, that is,

$$\frac{\partial^2 \hat{u}_i}{\partial q_i^2} \leq 0,$$

and dominates the off-diagonal elements in terms of absolute value, that is,

$$\left|\frac{\partial^2 \hat{u}_i}{\partial q_i^2}\right| > \left|\frac{\partial^2 \hat{u}_i}{\partial q_i \partial q_j}\right|.$$

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

The homogeneity condition and the discussions around (A6), coupled with inequalities (A11) and (A12), imply that (4.6) is a sufficient condition for the uniqueness of the equilibrium.

Proof of Theorem 4.4

The proof of this theorem also relies on Rosen (1965) and is largely similar to the proof in the previous theorem. A sufficient condition for $J + J^\intercal$ to be negative definite is that for all $i \in \{1, \dots, d\}$,

$$\frac{\partial^2 \hat{u}_i}{\partial q_i^2} \leq 0,$$

and U is strictly diagonally dominant, that is,

$$\left| \frac{\partial^2 \hat{u}_i}{\partial q_i^2} \right| > \frac{1}{2} \sum_{j=1, j \neq i}^{d} \left| \frac{\partial^2 \left(\hat{u}_i + \hat{u}_j \right)}{\partial q_i \partial q_j} \right| .$$

The non-negativity of $\frac{\partial^2 \hat{u}_i}{\partial q_i^2}$ under (4.7) can be observed from the discussions around (A6). Substituting inequalities (A11) and (A12) in the second inequality above leads to the sufficient condition (4.7) for the uniqueness of the equilibrium.

Proof of Proposition 4.2

Under the homogeneity condition in Theorem 4.3, there exists a unique Nash equilibrium. Furthermore, under the symmetry condition, the firms' objective functions are interchangeable, implying that, in this Nash equilibrium, all firms must have the same security level q^N. Otherwise, multiple equilibria would arise.

Recall that in the proof of Theorem 4.3, we have shown that the matrix with the (i, j)th element given by $\frac{\partial^2 \left(\hat{u}_i + \hat{u}_j \right)}{\partial q_i \partial q_j}$ for any pairs (i, j), $i, j \in \{1, \dots, d\}$, is negative definite. Thus, the Hessian matrix of $\hat{u}_S\,(q)$, which has the (i, j)th element given by $\frac{\partial^2 \left(\sum_k \hat{u}_k \right)}{\partial q_i \partial q_j}$, is also negative definite. This implies that $\hat{u}_S\,(q)$ is a concave function and, therefore, has only one unique maximum. Again, due to the interchangeability of the firms' objective functions, this maximum must be achieved with a uniform security level q^S; otherwise, multiple maxima would arise.

Notice also that, at the Nash equilibrium, the first derivative of $\hat{u}_S\,(q)$ with respect to q_i is given by:

$$\left. \frac{\partial \hat{u}_S}{\partial q_i} \right|_{q_1 = \cdots = q_d = q^N} = \left. \frac{\partial \hat{u}_i}{\partial q_i} \right|_{q_1 = \cdots = q_d = q^N} + \sum_{j \neq i} \left. \frac{\partial \hat{u}_j}{\partial q_i} \right|_{q_1 = \cdots = q_d = q^N} .$$

Due to the Nash equilibrium condition, the first term on the right-hand side above is zero. For the second term, (3.2) shows that an increase in the security level of firm j decreases the probability of firm i eventually being compromised. This implies that $\frac{\partial u_j}{\partial q_i} \geq 0$, and furthermore, $\frac{\partial \hat{u}_j}{\partial q_i} \geq 0$. Therefore, at the unique, symmetric Nash equilibrium $q = (q^N, \dots, q^N)$, the social welfare function $\hat{u}_S(q)$ is non-decreasing in each q_i, $i \in \{1, \dots, d\}$, implying $q^N \leq q^S$.

Proof of Proposition 4.3

Without loss of generality, assume there is a linkage between firms i and j. With $a_i^N, a_j^N, q_i^N, q_j^N < 1$, consider a small increase $\Delta q \in \left(0, 1 - \max\{q_i^N, q_j^N\}\right)$ from the security levels in the Nash equilibrium, that is, $\left(q_i^N + \Delta q, q_j^N + \Delta q\right)$, while keeping the insurance coverage ratios unchanged at a^N. Then, the difference in firm i's objective function, evaluated at this new profile versus the Nash equilibrium profile, is given by

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press

$$
\begin{aligned}
& u_i\left(a_i^N, q_1^N, \ldots, q_i^N + \Delta q, \ldots, q_j^N + \Delta q, \ldots, q_d^N\right) - u_i\left(a_i^N, q^N\right) \\
= & \left.\frac{\partial u_i}{\partial q_i}\right|_{(a,q)=\left(a^N, q^N\right)} \times \Delta q + \left.\frac{\partial u_i}{\partial q_j}\right|_{(a,q)=\left(a^N, q^N\right)} \times \Delta q + o\left(\Delta q\right) \\
= & \left.\frac{\partial u_i}{\partial q_j}\right|_{(a,q)=\left(a^N, q^N\right)} \times \Delta q + o\left(\Delta q\right).
\end{aligned}
$$

The partial derivative of u_i with respect to q_j is given by

$$
\frac{\partial u_i}{\partial q_j} = \left(1 - q_i\right) Q_{ij}\left(\mathbb{E}\left[U_i\left(W_i\right)\right] - \mathbb{E}\left[U_i\left(W_i - (1-a_i)L_i\right)\right]\right),
$$

which is strictly positive when $a_i, q_i < 1$ and firms i and j are linked, given the fundamental assumption that the variables W_i and L_i are not degenerate. Therefore, for suitably small but positive Δq, firm i's objective function is higher at the new security profile $\left(q_i^N + \Delta q, q_j^N + \Delta q\right)$, and the same can be shown for firm j. The utilities of the firms in $\{1, \ldots, d\}\backslash\{i, j\}$ weakly increase as well because $\Delta q > 0$. In conclusion, we have identified a strategy profile that Pareto dominates the Nash equilibrium, and thus, the Nash equilibrium is not Pareto efficient.

https://doi.org/10.1017/asb.2024.40 Published online by Cambridge University Press