On Equilibrium Cyber Risk[*]

Carlos A. Ramírez

October 28, 2024

Abstract

I develop a simple model to study how the interplay between the incentives of institutions and hackers alters cyber risk in equilibrium. The model shows that larger institutions are more likely to be targeted in economies wherein hackers' payoffs are proportional to the size of their targets. The model also highlights how changes in cybersecurity technologies and competition among hackers can reshape the distribution of cyberattacks, leading to significant shifts in cyber risk.

JEL Codes: D39, D22, M15.
Keywords: equilibrium cyber risk, cybersecurity, cyberattacks, hacks.

Highlights:

- The model offers an explanation of why hackers target larger institutions.
- The distribution of cyberattacks across institutions is closely linked to their size distribution.
- Smaller institutions become more likely targets as cybersecurity technologies improve or competition among hackers intensifies.

[*] Federal Reserve Board. These are my views and do not necessarily reflect those of the Federal Reserve Board or other members of its staff. Email: carlos.ramirez@frb.gov. There are no competing interests to declare.

1 Introduction

In recent years, cyber risk has become a pressing concern for businesses, market participants, regulators, and academics alike.[1] Yet much of the existing literature overlooks equilibrium considerations in its assessments. Simply put, hackers' behavior is likely shaped by their expectations of institutions' investments in cybersecurity, while institutions base their actions on anticipated hackers' choices. This oversight stems from the difficulties in observing hackers' motivations and institutional responses as well as the lack of consensus on how these factors interact to determine the equilibrium distribution of cyberattacks in an economy.[2] To fill this gap, I propose a simple model to connect the motivations of hackers and institutions within an equilibrium framework, offering a clearer understanding of how basic characteristics of an economy can reshape cyber risk.

The proposed model has two main features. First, institutions and hackers (motivated solely by financial gain) would like to outguess one another before making decisions. Second, hackers' rewards are proportional to the size of their targets, reflecting the idea that larger institutions might be capable of paying higher ransoms. With this model in hand, I characterize its equilibrium and establish a mapping between the distribution of cyberattacks and the size distribution of institutions. Importantly, this mapping can be reshaped by the severity of hacks and the intensity of competition among hackers.

Consistent with recent empirical evidence (see Chang et al. (2024)), I show that larger institutions are frequently targeted in equilibrium due to the higher potential rewards associated with larger targets. In addition, I show that smaller institutions become more attractive targets as cybersecurity technologies improve or competition among hackers intensifies. This shift occurs because rewards from targeting larger institutions decrease as hacks become less severe or competition intensifies, prompting hackers to redirect their efforts to smaller institutions.

My results contribute to the rapidly expanding literature on the drivers and potential consequences of cyber risk. For example, Aldasoro et al. (2020) and Chang et al. (2024) document an empirical relationship between the size of institutions and the likelihood

[1] The following reports underscore concerns of business leaders and regulators about the systemwide repercussions of cyberattacks and measures taken to strengthen cybersecurity within the financial sector: World Economic Forum Report and Federal Reserve Board Report. This IMF blog also highlights the rising threats to financial stability stemming from cyberattacks.

[2] See Ablon (2018) and Chng et al. (2022) for a description of hackers' motivations.

of cyberattacks. Jamilov et al. (2021), Kamiya et al. (2021), Florackis et al. (2023), and Jiang et al. (2024) underscore the impact of cyber risk on stock returns, while Curti et al. (2023) show that hacks affecting state and local governments can increase their financing costs.[3] Although my work shares with these papers its focus on either the distribution of cyberattacks or how such incidents influence institutional decisions, to the best of my knowledge, my paper is the first to conceptually explore how the interplay between the incentives of both institutions and hackers alters cyber risk in equilibrium. In doing so, my paper provides a simple model to which other frameworks can be compared.

2 The Hacking Game

Consider an economy consisting of a unit continuum of institutions (firms, for short), each varying in size, alongside a single hacker motivated solely by financial gain. I focus on simple games wherein firms and the hacker choose their actions simultaneously, and payoffs (which are common knowledge) depend on the combination of selected actions.

For simplicity, consider a firm of size $s \in (0, 1)$ and the hacker. The proposed game—referred to as the hacking game—shares a distinguishing feature with the game of Matching Pennies: both players, the firm and the hacker, would like to outguess one another.[4] The firm would like to anticipate whether the hacker will attack before deciding how much to invest in cybersecurity, while the hacker would like to know how much the firm invests in cybersecurity before allocating resources to the attack. Because the solution of this game involves uncertainty about what players will do, let q_s denote the probability that a firm of size s chooses to defend itself and p_s denote the probability that the hacker chooses to target that firm.

For a given tuple (q_s, p_s), Table 1 reports players' payoffs.[5] To reflect the idea that larger firms may be capable of paying higher ransoms, I assume that the hacker's rewards are proportional to the size of targeted firms. Parameter $\alpha \in (0, 1)$ is inversely related to

[3] Another related literature emphasizes how individual hacks can impair important sectors of the economy via propagation along supply chains, payment systems, or technology providers (see Eisenbach et al. (2022), Kotidis and Schreft (2022), Crosignani et al. (2023)), while Duffie and Younger (2019) and Kashyap and Wetherilt (2019) highlight the potential systemwide implications of cyberattacks and the policy challenges that stem from them.

[4] See (Gibbons, 1992, chap 1.3).

[5] In any game in which each player would like to outguess the other, there is no Nash equilibrium in pure strategies, as the solution involves uncertainty about what players will do. Therefore, analyzing mixed strategies is critical when solving for equilibria.

Hacker $\mid$ Firm of size s	Defend with prob. q_s	Do not defend with prob. $(1-q_s)$
Attack with prob. p_s	Hacker: $\frac{(1-\alpha)s}{2} - p_s$ Firm: $\alpha s + \frac{(1-\alpha)s}{2} - q_s$	Hacker: $(1-\alpha)s - p_s$ Firm: αs
Do not attack with prob. $(1-p_s)$	Hacker : 0 Firm: $s - q_s$	Hacker : 0 Firm: s

Table 1: Matrix of payoffs

the severity of successful hacks. As α decreases, firms obtain lower payoffs when targeted, while the hacker obtains higher rewards.

Intuitively, firms prefer not to defend themselves if the hacker does not attack; yet if the hacker attacks, firms would opt to defend. While firms obtain higher payoffs when there is no attack, the hacker gains nothing from abstaining. To account for the costs associated with cyberattacks and cybersecurity investments, variables (q_s, p_s) can modify the above payoffs. As a result, these variables might also be interpreted as the intensity of players' actions: q_s can be thought of as how aggressively a firm of size s invests in cybersecurity, while p_s can be thought of as the intensity of the hack on that firm. Incorporating this feature not only enriches the model, but also ensures the uniqueness of the equilibrium by enforcing concavity in the expected payoff of both players.

Best Response Functions.—Consider (q_s, p_s) as choice variables. Solving for the first-order conditions of the firm and the hacker yields the following best response functions:

$$q^*(p_s) = \left(\frac{1-\alpha}{4}\right) s \times p_s \quad \text{and} \quad p^*(q_s) = \left(\frac{1-\alpha}{2}\right) s \times \left(1 - \frac{q_s}{2}\right). \tag{1}$$

That is, a firm's best response, $q^*(\cdot)$, increases with its size, s, the likelihood/intensity of being targeted, p_s, and the severity of hacks (as lower values of α are associated with more severe hacks). In turn, the hacker's best response, $p^*(\cdot)$, increases with the size of targeted firms and the severity of hacks, and it decreases with the likelihood/intensity of firms defending themselves.

Equilibrium.—In equilibrium, players maximize their expected payoffs, with no player having unilateral incentives to deviate. Consequently, the strategies of firms and the hacker are best responses to one another. The following proposition demonstrates that the hacking game has a unique equilibrium.

PROPOSITION 1 *The simultaneous move game between the hacker and the unit* *continuum of firms has a unique equilibrium. In such equilibrium, a firm of size s faces a targeting probability of p_s^e while investing q_s^e in cybersecurity, where*

$$p_s^e = \frac{(1-\alpha)s}{2\left(1+\frac{(1-\alpha)^2}{16}s^2\right)} \quad \textit{and} \quad q_s^e = \frac{(1-\alpha)^2 s^2}{8\left(1+\frac{(1-\alpha)^2}{16}s^2\right)}. \tag{2}$$

That is, the equilibrium distribution of cyberattacks is intimately linked to the distribution of firm sizes and reshaped by the severity of hacks. Importantly, p_s^e and q_s^e reflect both (1) the hacker's understanding that firms invest more in cybersecurity when the risk of being targeted is higher as well as (2) firms' understanding that increasing cybersecurity investments discourages the hacker from targeting them.

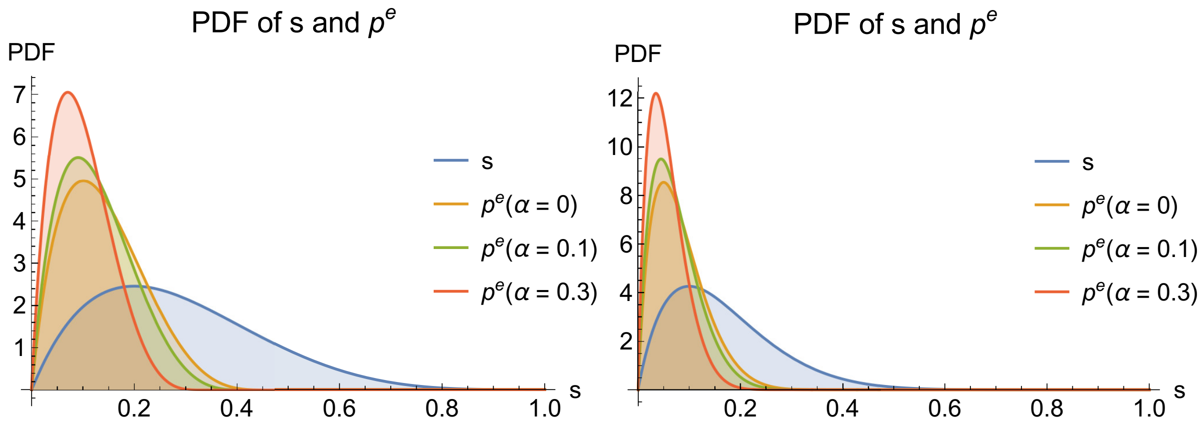
Equilibrium Characteristics.—Lemma 1 describes how firms' sizes and the severity of hacks can alter the likelihood of being targeted in equilibrium.

LEMMA 1 *p_s^e increases with s and decreases with α. And $\frac{\partial^2 p_s^e}{\partial s \partial \alpha}$ is negative.*

Lemma 1 highlights three key characteristics of equilibrium behavior. First, p_s^e is an increasing function of s. Consistent with recent empirical evidence (see Chang et al. (2024)), the hacker targets larger firms in equilibrium. Although larger firms invest more in cybersecurity, the hacker still benefits from targeting them as her rewards are proportional to the size of her targets. Second, p_s^e is a decreasing function of α. As the severity of hacks increases, so do the hacker's rewards, thereby increasing her incentives to attack. Third, $\frac{\partial p_s^e}{\partial \alpha}$ becomes more negative as s increases. Intuitively, in the face of a marginal increase in the severity of hacks, larger firms experience a more pronounced increase in their likelihood of being targeted compared to smaller firms. This result also stems from the fact that the hacker's rewards are proportional to the size of her targets.

Illustrative Examples.—To help appreciate Proposition 1, assume that the size distribution of firms follows a Beta distribution with long right tails, making it comparable to the size distribution across U.S. firms. Figure 1 depicts the distribution of s and p_s^e under various parameter configurations. Panel (a) assumes $s \sim \beta(2, 5)$, while panel (b) assumes $s \sim \beta(2, 10)$ to emphasize the relevance of longer tails.

Both panels of figure 1 illustrate that the precise functional form of firms' size distribution plays a critical role in the distribution of cyberattacks, thereby reshaping cyber risk in equilibrium. The severity of hacks is also crucial: As firms become better at defending themselves (higher α), hacks become more concentrated, leading to a decrease



(a) $s \sim \beta(2, 5)$

(b) $s \sim \beta(2, 10)$

Figure 1: Firm size distribution and targeting probabilities

in the average size of targeted firms. Intuitively, smaller firms invest relatively less in cybersecurity, making them more appealing targets as cybersecurity technologies improve. In addition, as the juxtaposition of both panels of figure 1 show, the size of the average targeted firm decreases as firms become more heterogeneous in size (longer tails). As larger firms become less common, the hacker shifts her focus to smaller firms, resulting in a reduction of the average size of her targets.

3 The Hacking Game with Competition

Although the previous analysis sheds light on how individual incentives can influence cyber risk within an equilibrium framework, it fails to account for the fact that multiple hackers might coexist. This section explores how competition among hackers can modify the incentives for both firms and hackers, ultimately reshaping equilibrium cyber risk.

For tractability, hereinafter I focus on symmetric equilibria wherein every hacker chooses the same strategy. Besides a unit continuum of firms of varying sizes, the economy consists of n hackers that compete among each other when targeting firms. Table 2 reports the payoffs of hackers and firms in an extended version of the hacking game. Reported payoffs consider a firm of size s and a single hacker. Panel A assumes that the remaining $(n - 1)$ hackers choose to attack, while panel B assumes that the remaining hackers choose not to attack. As before, q_s represents the probability/intensity that a firm of size s chooses to defend itself, while p_s denotes the probability/intensity that a single hacker chooses to target that firm.

Panel A: remaining $(n-1)$ hackers attack

Hacker $\mid$ Firm of size s	Defend with prob. q_s	Do not defend with prob. $(1-q_s)$
Attack with prob. p_s	Hacker: $\frac{(1-\alpha)s}{2n} - p_s$ Firm: $\alpha s + \frac{(1-\alpha)s}{2} - q_s$	Hacker: $\frac{(1-\alpha)s}{n} - p_s$ Firm: αs
Do not attack with prob. $(1-p_s)$	Hacker : 0 Firm: $\alpha s + \frac{(1-\alpha)s}{2} - q_s$	Hacker : 0 Firm: αs

Panel B: remaining $(n-1)$ hackers do not attack

Hacker $\mid$ Firm of size s	Defend with prob. q_s	Do not defend with prob. $(1-q_s)$
Attack with prob. p_s	Hacker: $\frac{(1-\alpha)s}{2} - p_s$ Firm: $\alpha s + \frac{(1-\alpha)s}{2} - q_s$	Hacker: $(1-\alpha)s - p_s$ Firm: αs
Do not attack with prob. $(1-p_s)$	Hacker : 0 Firm: $s - q_s$	Hacker : 0 Firm: s

Table 2: Matrix of payoffs with competition among hackers

In addition to assuming that hackers' rewards are proportional to the size of targeted firms, I assume that hackers equally share the rewards from successful attacks. Although this assumption is not essential, it simplifies calculations by removing equilibrium considerations associated with heterogeneity in bargaining power among hackers. To further simplify exposition, I assume that a firm's payoffs are independent of the number of hackers. The Online Appendix shows that my results continue to hold even when a firm's payoffs depend on the precise number of hackers operating in the economy.

Competition and Cybersecurity Strategies.—Solving for the firm's first-order condition yields the following best response function:

$$q^*(p_s) \quad = \quad \left(\frac{1-\alpha}{4}\right) s \times \left(\frac{p_s^{n-1} + p_s(1-p_s)^{n-1}}{p_s^{n-1} + p_s(1-p_s)^{n-1} + (1-p_s)^n}\right). \tag{3}$$

As before, a firm's cybersecurity response, q^*, increases with both its size, s, and the severity of hacks. While q^* also increases with the likelihood/intensity of being targeted, p_s, the relationship between q^* and p_s is reshaped by the intensity of competition among hackers, n. As competition intensifies—that is, n grows—

$$\lim_{n\to\infty} q^*(p_s) \quad = \quad \begin{cases} \left(\frac{1-\alpha}{4}\right) s \times p_s & \text{if } p_s \leq 1/2, \\ \left(\frac{1-\alpha}{4}\right) s & \text{otherwise.} \end{cases} \tag{4}$$

That is, as the number of hackers grows large, firms either act as if they are almost surely targeted or as if they face a single hacker.

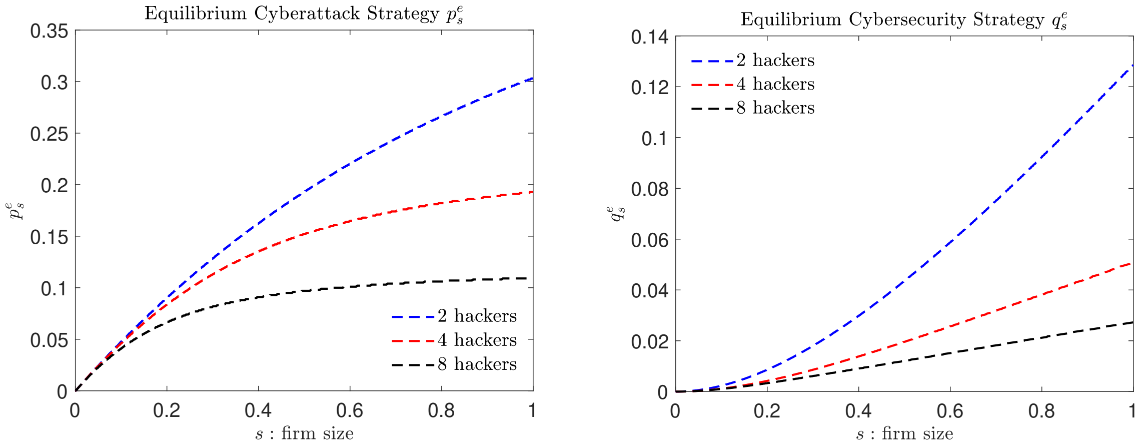
Equilibrium.—In equilibrium, hackers and firms maximize their expected payoffs, with no player having unilateral incentives to deviate. The following proposition demonstrates that the hacking game with competition has a unique symmetric equilibrium.

PROPOSITION 2 *The simultaneous move game between n hackers and the unit continuum of firms has a unique symmetric equilibrium. In such equilibrium, a firm of size s invests q_s^e in cybersecurity, where*

$$q_s^e = \left(\frac{1-\alpha}{4}\right) s \times \left(\frac{(p_s^e)^{n-1} + p_s^e(1-p_s^e)^{n-1}}{(p_s^e)^{n-1} + p_s^e(1-p_s^e)^{n-1} + (1-p_s^e)^n}\right), \tag{5}$$

and $p_s^e = \text{argmax}\, \mathbb{E}[\pi^{hacker}(p_s)|q^*(p_s) = q_s^e]$ maximizes the expected payoff of an arbitrary hacker targeting such firm.

That is, competition among hackers can also modify the equilibrium distribution of cyberattacks and, thus, cyber risk.



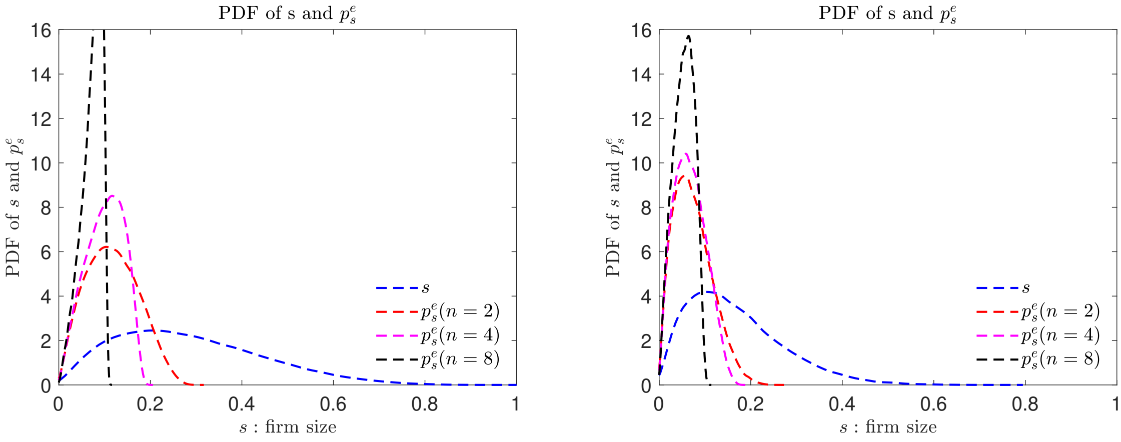
(a) p_s^e

(b) q_s^e

Figure 2: p_s^e and q_s^e when $n \in \{2, 4, 8\}$ and $\alpha = 0$.

To illustrate Proposition 2, figure 2 depicts p_s^e and q_s^e for different values of n, assuming $\alpha = 0$. Panel A shows that, as before, p_s^e increases with a firm's size. Thus, results with competition are also aligned with recent empirical evidence. Notably, increased competition makes larger firms less likely to be targeted, as a hacker's payoffs decrease as competition intensifies. Because rewards from successful hacks are proportional to firm size, such a decrease is more pronounced among larger firms. Consequently, it becomes optimal for hackers to target smaller firms as competition intensifies. Panel B depicts the optimal cybersecurity strategy as a function of firms' size. As before, larger firms invest more in cybersecurity. Yet all firms invest less as n grows. In the face of increased competition, hackers receive smaller rewards from hacks, reducing their incentives to attack. Recognizing this effect, firms preemptively invest less in cybersecurity.

Illustrative Examples.—To illustrate the importance of Proposition 2, assume that firms size follows a Beta distribution with long right tails. Panel A of figure 3 assumes $s \sim \beta(2, 5)$, while panel B assumes $s \sim \beta(2, 10)$.



(a) $s \sim \beta(2, 5)$ and $\alpha = 0$

(b) $s \sim \beta(2, 10)$ and $\alpha = 0$

Figure 3: Impact of hacker competition on targeting probabilities

As figure 3 shows, the size of the average targeted firm as well as the variance of p_s^e decreases as hacker competition intensifies.

Competition and Cyber Risk.— In sum, competition modifies the incentives of firms and hackers, leading to changes in the equilibrium distribution of cyberattacks and, hence, cyber risk. As competition increases, firms invest less in cybersecurity as they understand that hackers have less incentives to target them. This effect is especially important among larger firms.

4 Conclusion

I develop a model to study how cyber risk is influenced by the motivations of firms and hackers. Aligned with recent empirical evidence, my model shows that larger firms are more frequently targeted. Additionally, my model establishes a clear relationship between the distribution of firm sizes and the likelihood of cyberattacks, highlighting that smaller firms become increasingly attractive targets as cybersecurity technologies improve or competition among hackers intensifies. My findings underscore the importance of understanding the interplay between the motivations of firms and hackers when assessing cyber risk.

References

Ablon, Lillian, 2018, Data thieves: The motivations of cyber threat actors and their use and monetization of stolen data, Testimony presented before the House Financial Services Committee, Subcommittee on Terrorism, and Illicit Finance, on March 15, 2018.

Aldasoro, Iñaki, Leonardo Gambacorta, Paolo Giudici, and Thomas Leach, 2020, The drivers of cyber risk, *BIS Working Paper* .

Chang, Jin-Wook, Kartik Jayachandran, Carlos A. Ramírez, and Ali Tintera, 2024, On the anatomy of cyberattacks, *Economics Letters* 238, 111676.

Chng, Samuel, Han Yu Lu, Ayush Kumar, and David Yau, 2022, Hacker types, motivations and strategies: A comprehensive framework, *Computers in Human Behavior Reports* 5, 100167.

Crosignani, Matteo, Marco Macchiavelli, and André F. Silva, 2023, Pirates without borders: The propagation of cyberattacks through firms' supply chains, *Journal of Financial Economics* 147, 432–448.

Curti, Filippo, Ivan Ivanov, Marco Macchiavelli, and Tom Zimmermann, 2023, City hall has been hacked! the financial costs of lax cybersecurity, *Mimeo* .

Duffie, Darrell, and Joshua Younger, 2019, Cyber runs: How a cyber attack could affect u.s. financial institutions, *Hutchins Center Working Paper* 51.

Eisenbach, Thomas M., Anna Kovner, and Michael Junho Lee, 2022, Cyber risk and the u.s. financial system: A pre-mortem analysis, *Journal of Financial Economics* 145, 802–826.

Florackis, Chris, Christodoulos Louca, Roni Michaely, and Michael Weber, 2023, Cybersecurity risk, *Review of Financial Studies* 36, 351–407.

Gibbons, Robert, 1992, *Game Theory for Applied Economists* (Princeton University Press).

Jamilov, Rustam, Hélene Rey, and Ahmed Tahoun, 2021, The anatomy of cyber risk, *NBER Working Paper Series* .

Jiang, Hao, Naveen Khanna, Qian Yang, and Jiayu Zhou, 2024, The cyber risk premium, *Management Science* .

Kamiya, Shinichi, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and Rene M. Stulz, 2021, Risk management, firm reputation, and the impact of successful cyberattacks on target firms, *Journal of Financial Economics* 139, 719–749.

Kashyap, Anil K., and Anne Wetherilt, 2019, Some principles for regulating cyber risk, *AEA Papers and Proceedings* 109, 482–487.

Kotidis, Antonis, and Stacey L. Schreft, 2022, Cyberattacks and financial stability: Evidence from a natural experiment, *Finance and Economics Discussion Series (FEDS)* .

Online Appendix for
"On Equilibrium Cyber Risk"

This Appendix contains material to supplement the analysis in "On Equilibrium Cyber Risk." Section A provides proofs of the two propositions and lemma in the main text. Section B describes an extension of the baseline model and shows that my central findings continue to hold even when firms' payoffs depend on the precise number of hackers operating in an economy.

A Proofs

A.1 Economies with a single hacker

I first analyze the best response of firms and then explore the best response of the hacker.

Given p_s, the expected payoff of a firm of size s equals

$$\mathbb{E}[\pi^{\text{firm}}(q_s)|p_s] \quad = \quad p_s \left\{ q_s \left(\frac{1+\alpha}{2}s - q_s \right) + (1-q_s)\alpha s \right\} + (1-p_s)\left\{ q_s(s-q_s) + (1-q_s)s \right\}$$

which is concave on q_s. The first order condition of such firm then equals

$$p_s \left(\frac{1-\alpha}{2}s - 2q_s \right) - 2q_s(1-p_s) \quad = \quad 0. \tag{1}$$

Consequently, the best response function of such firm is

$$q_s^*(p_s) \quad = \quad \frac{1-\alpha}{4}sp_s. \tag{2}$$

Suppose the hacker targets a firm of size s. Given q_s, the expected payoff of the hacker equals

$$\mathbb{E}[\pi^{\text{hacker}}(p_s)|q_s] \quad = \quad p_s \left\{ q_s \left(\frac{1-\alpha}{2}s - p_s \right) + (1-q_s)[(1-\alpha)s - p_s] \right\}$$

which is concave on p_s. The first order condition of the hacker then equals

$$q_s \left(\frac{1-\alpha}{2}s - p_s \right) + (1-q_s)[(1-\alpha)s - p_s] \quad = \quad p_s. \tag{3}$$

As a result, the best response function of the hacker is

$$p_s^*(q_s) \quad = \quad \frac{1-\alpha}{2}s\left(1 - \frac{q_s}{2}\right). \tag{4}$$

Proof of Proposition 1 In equilibrium no player has unilateral incentives to deviate as players behave according to their best response functions. The equilibrium then corresponds to any point wherein functions $q_s^*(p_s)$ and $p_s^*(q_s)$ intersect with one another. If such point exists, it is then unique as these functions are linear in their arguments.

The solution of the system of equations (2) and (4) is then

$$p_s^e = \frac{(1-\alpha)s}{2\left(1+\frac{(1-\alpha)^2}{16}s^2\right)} \quad \text{and} \quad q_s^e = \frac{(1-\alpha)^2 s^2}{8\left(1+\frac{(1-\alpha)^2}{16}s^2\right)}. \tag{5}$$

Proof of Lemma 1 Note that

$$\frac{\partial p_s^e}{\partial s} = \frac{8(1-\alpha)(16-(1-\alpha)^2 s^2)}{(16+(1-\alpha)^2 s^2)^2} \quad \text{and} \quad \frac{\partial p_s^e}{\partial \alpha} = \frac{8s((1-\alpha)^2 s^2 - 16)}{(16+(1-\alpha)^2 s^2)^2}. \tag{6}$$

Because α and s are between zero and one, the derivative of the term on the left hand side in (6) is positive while the derivative of the term on the right hand side is negative. For the same reason, the following cross-derivative

$$\frac{\partial^2 p_s^e}{\partial s \partial \alpha} = -\frac{8(256-96(1-\alpha)^2 s^2 + s^4(1-\alpha)^4)}{(16+(1-\alpha)^2 s^2)^3} \tag{7}$$

is negative.

A.2 Economies with multiple hackers

As before, I first analyze the best response of firms and then explore the best response of hackers. To facilitate exposition, I solely focus on symmetric equilibria wherein every hacker selects the same strategy.

Given p_s, the expected payoff of a firm of size s equals

$$\begin{aligned}
\mathbb{E}[\pi^{\text{firm}}(q_s)|p_s] &= p_s^{n-1}\left(p_s\left\{q_s\left(\frac{1+\alpha}{2}s - q_s\right) + (1-q_s)\alpha s\right\}\right) \\
&+ p_s^{n-1}\left((1-p_s)\left\{q_s\left(\frac{1+\alpha}{2}s - q_s\right) + (1-q_s)\alpha s\right\}\right) \\
&+ (1-p_s)^{n-1}\left(p_s\left\{q_s\left(\frac{1+\alpha}{2}s - q_s\right) + (1-q_s)\alpha s\right\}\right) \\
&+ (1-p_s)^{n-1}\left((1-p_s)\left\{q_s(s-q_s) + (1-q_s)s\right\}\right),
\end{aligned}$$

which is concave on q_s. The first order condition of such firm then equals

$$\left[p_s^{n-1} + p_s(1-p_s)^{n-1}\right]\left(\frac{1-\alpha}{2}s - 2q_s\right) - 2q_s(1-p_s)^n = 0. \tag{8}$$

Consequently, the best response function of such firm is

$$\begin{aligned}
q_s^*(p_s) &= \left(\frac{1-\alpha}{4}\right)s \times \left(\frac{p_s^{n-1} + p_s(1-p_s)^{n-1}}{p_s^{n-1} + p_s(1-p_s)^{n-1} + (1-p_s)^n}\right) \\
&= \underbrace{\left(\frac{1-\alpha}{4}\right)}_{A(s)} s \times \left(\frac{1}{1+\frac{(1-p_s)^n}{p_s^{n-1}+p_s(1-p_s)^{n-1}}}\right).
\end{aligned} \tag{9}$$

Taking the limit of equation (9) when n grows yields

$$\lim_{n\to\infty} q_s^*(p_s) = A(s) \times \left(\frac{1}{1 + \frac{(1-p_s)^n}{p_s^{n-1}+p_s(1-p_s)^{n-1}}} \right) = \begin{cases} A(s) \times p_s & \text{if } p_s \leq 1/2, \\ A(s) & \text{otherwise.} \end{cases} \tag{10}$$

That is, when the number of hackers in the economy grows large, firms either act as if they are almost surely targeted or as if they face a single hacker.

Proof of Proposition 2 As previously mentioned, no player has unilateral incentives to deviate in equilibrium as they behave according to their best response functions. Then, the equilibrium of the simultaneous move game between n hackers and the unit continuum of firms corresponds to any point wherein functions $q_s^*(p_s)$ and $p_s^*(q_s)$ intersect with one another—where $p_s^*(q_s)$ maximizes the expected payoff of an arbitrary hacker targeting a firm of size s. Because α and s are between zero and one, the following optimization problem

$$\max_{0\leq p_s \leq 1} \mathbb{E}[\pi^{\text{hacker}}(p_s)|q_s = q_s^*(p_s)], \tag{11}$$

has a unique solution. As a result, the simultaneous move game with multiple hackers has a unique symmetric equilibrium.

B Robustness

This section describes a variation of the baseline model with multiple hackers wherein firms' payoffs now depend on the precise number of hackers in the economy. As before, besides the unit continuum of firms of varying sizes, there are n hackers that compete among each other when targeting firms.

Table 1 reports players' payoffs

Panel A: remaining $(n-1)$ hackers attack

Hacker | Firm of size s	Defend with prob. q_s	Do not defend with prob. $(1-q_s)$
Attack with prob. p_s	Hacker: $\frac{(1-\alpha)s}{n+1} - p_s$ Firm: $\alpha s + \frac{(1-\alpha)s}{n+1} - q_s$	Hacker: $\frac{(1-\alpha)s}{n} - p_s$ Firm: αs
Do not attack with prob. $(1-p_s)$	Hacker : 0 Firm: $\alpha s + \frac{(1-\alpha)s}{n} - q_s$	Hacker : 0 Firm: αs

Panel B: remaining $(n-1)$ hackers do not attack

Hacker | Firm of size s	Defend with prob. q_s	Do not defend with prob. $(1-q_s)$
Attack with prob. p_s	Hacker: $\frac{(1-\alpha)s}{2} - p_s$ Firm: $\alpha s + \frac{(1-\alpha)s}{2} - q_s$	Hacker: $(1-\alpha)s - p_s$ Firm: αs
Do not attack with prob. $(1-p_s)$	Hacker : 0 Firm: $s - q_s$	Hacker : 0 Firm: s

Table 1: Matrix of payoffs with competition among hackers

That is, firms do care about the precise number of hackers attacking them; previously that number did not matter. The reason is that potential rewards are now equally shared between hackers and the firm should the firm decide to defend itself.

In this environment, the best response function of a firm of size s equals

$$q_s^*(p_s) \quad = \quad \left(\frac{1-\alpha}{2}\right) s \times \left(\frac{\frac{p_s^n}{n+1} + \frac{(1-p_s)p_s^{n-1}}{n} + \frac{p_s(1-p_s)^{n-1}}{2}}{p_s^n + (1-p_s)p_s^{n-1} + p_s(1-p_s)^{n-1} + (1-p_s)^n}\right). \tag{12}$$

Notably, taking the limit of equation (12) when n grows large yields

$$\lim_{n\to\infty} q_s^*(p_s) \quad = \quad \begin{cases} \frac{1-\alpha}{4} s \times p_s & \text{if } p_s \leq 1/2, \\ \frac{1-\alpha}{4} s & \text{otherwise.} \end{cases} \tag{13}$$

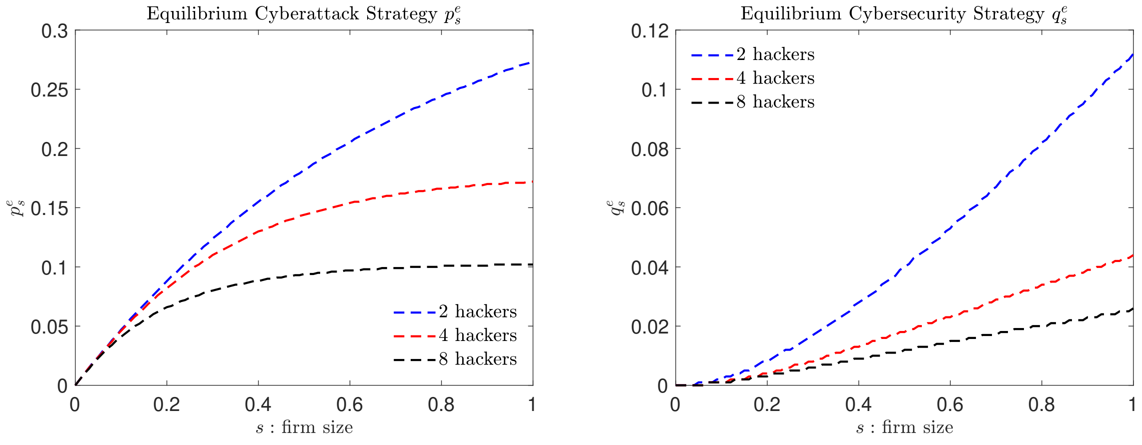
That is, when the number of hackers in the economy grows large, firms behave as they would behave in the hacking game with competition. That is, firms either act as if they are almost surely targeted or as if they face a single hacker.

The rationale behind the existence and uniqueness of the equilibrium of the simultaneous move game relies on the same idea as before. Because α and s are between zero and one, the following optimization problem

$$\max_{0\leq p_s\leq 1} \mathbb{E}[\pi^{\text{hacker}}(p_s)|q_s = q_s^*(p_s)], \tag{14}$$

has a unique solution. As a result, there is a unique symmetric equilibrium.

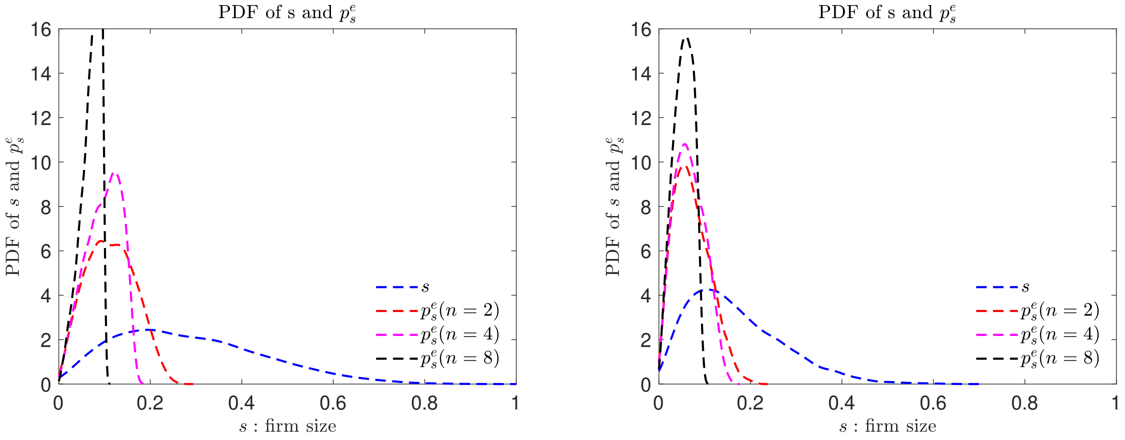
To emphasize the quantitative relevance of the change in payoffs, the following figures depict the analogs of figures 2 and 3 in the paper.



(a) p_s^e

(b) q_s^e

Figure 1: p_s^e and q_s^e when $n \in \{2, 4, 8\}$ and $\alpha = 0$ in the variation of the baseline model.



(a) $s \sim \beta(2,5)$ and $\alpha = 0$

(b) $s \sim \beta(2,10)$ and $\alpha = 0$

Figure 2: Impact of hacker competition on targeting probabilities in the variation of the baseline model.