unibz

Fakultät für Wirtschaftswissenschaften
Facoltà di Economia
Faculty of Economics and Management

BEMPS –
Bozen Economics & Management
Paper Series

NO 75/ 2020

Dangerous Games: A Literature Review on Cybersecurity Investments

Alessandro Fedele, Cristian Roner

Dangerous Games: A Literature Review on Cybersecurity Investments[*]

Alessandro Fedele[‡] and Cristian Roner[⋆]

[‡]*Free University of Bozen-Bolzano (Italy).*
alessandro.fedele@unibz.it
[⋆]*Free University of Bozen-Bolzano (Italy).*
cristian.roner@economics.unibz.it

Abstract

Cybersecurity has gained prominence in the decision-making of firms. Due to the increasing occurrences of threats in the cyberspace, investments in cybersecurity have become critical to mitigate the operational disruption of businesses. This paper surveys the theoretical literature on the firms' incentives to invest in cybersecurity. A taxonomy of the existing contributions is provided to frame them in a common reference scheme and a model is developed to encompass such contributions and discuss their main findings. Papers that investigate the investment problem of an isolated firm are distinguished from those that consider interdependent firms. In turn, interdependent cybersecurity is analyzed in three different contexts: (i) firms that operate their business via a common computer network, but are not competitors in the product market; (ii) firms that are competitors in the product market, but run their business using non-interconnected computer systems; (iii) firms that are competitors and rely on a common computer network. Promising avenues for future research are discussed in the conclusions.

Keywords: cybersecurity investments; interdependent cybersecurity; computer networks; product market competition.

JEL Classification: L86 (Information and Internet Services • Computer Software), M15 (IT Management), D81 (Criteria for Decision-Making under Risk and Uncertainty), C72 (Noncooperative Games), D62 (Externalities).

[*] We thank Rainer Böhme, the seminar audience at the Annual Conference of the Italian Economic Association (October 2020), and the 3rd Internal PhD Workshop at the Free University of Bozen-Bolzano for useful comments. The usual disclaimer applies.

1 Introduction

In the information technology (IT) industry, the concentration process triggered by network externalities and economies of scale (Tirole, 2017; Comino and Manenti, 2014) have made few corporations - one can think of the Big Five tech companies - the sole custodians of a large, centralized and growing pool of personal data. This phenomenon is not limited to the IT sector, as most firms and institutions manage an increasing amount of information essential to operate in a data-driven economy. For this reason, more and more often, they must confront with the threats of cyberattacks aimed at stealing information or causing damages. As a notable example, the fears over growing vulnerability to cyberattacks play a decisive role in the case of many Western countries against Chinese company Huawei building the infrastructures for the fifth generation of mobile network (UK Government, 2020a).[1]

Cyberbreaches may cause relevant monetary and reputational losses and can even compromise a firm business continuity altogether, with consequences reverberating throughout the economy. A recent report by Microsoft states that the total cost of cybercrime to the global economy in 2016 was as high as 500 billion USD and that 1 in 5 small and medium businesses are targeted in cyberattacks (Microsoft Corporation, 2016). Similarly, CSIS-McAfee (2018) estimates that the cybercrime costed the world economy between 445 and 608 billion USD in 2016, or about 0.6-0.8 percent of the global GDP; this is equivalent to a 14-percent tax on the Internet economy, which generated 4.2 trillion USD in 2016. These figures, however, are likely underestimating the true costs because they do not include, for instance, the work hours needed to counter an attack and restore a system after a breach, or long-term effects such as the loss of share value, the reputation damage, fines from authorities, and legal costs (Biancotti and Cristadoro, 2018). Moreover, firms tend to withhold information on cyberattacks (Amir et al., 2018).

The occurrence of data breaches and the related costs show an upward trend. Figure 1 reports the number of cyberbreaches and the millions of data records thereby exposed in the US over the last 15 years.[2] While the number of breaches raised on average by 22.8 percent, the data records exposed increased by 130.7 percent.[3] The average nominal costs due to reported cybercrimes worldwide are almost 200 times higher in 2019 than they were in 2001 (Statista on FBI data, 2020); a recent study by IBM on more than 500 cases of cyberbreaches around the world estimates an average cost of about 3.9 million USD, showing a 10 percent increase over the last six years (IBM Corporation, 2020). The growing trend of cyberbreaches and related costs is likely to be further fuelled by the enduring low awareness about cybersecurity among small and medium businesses (Paulsen, 2016; Ponemon Institute, 2019; UK

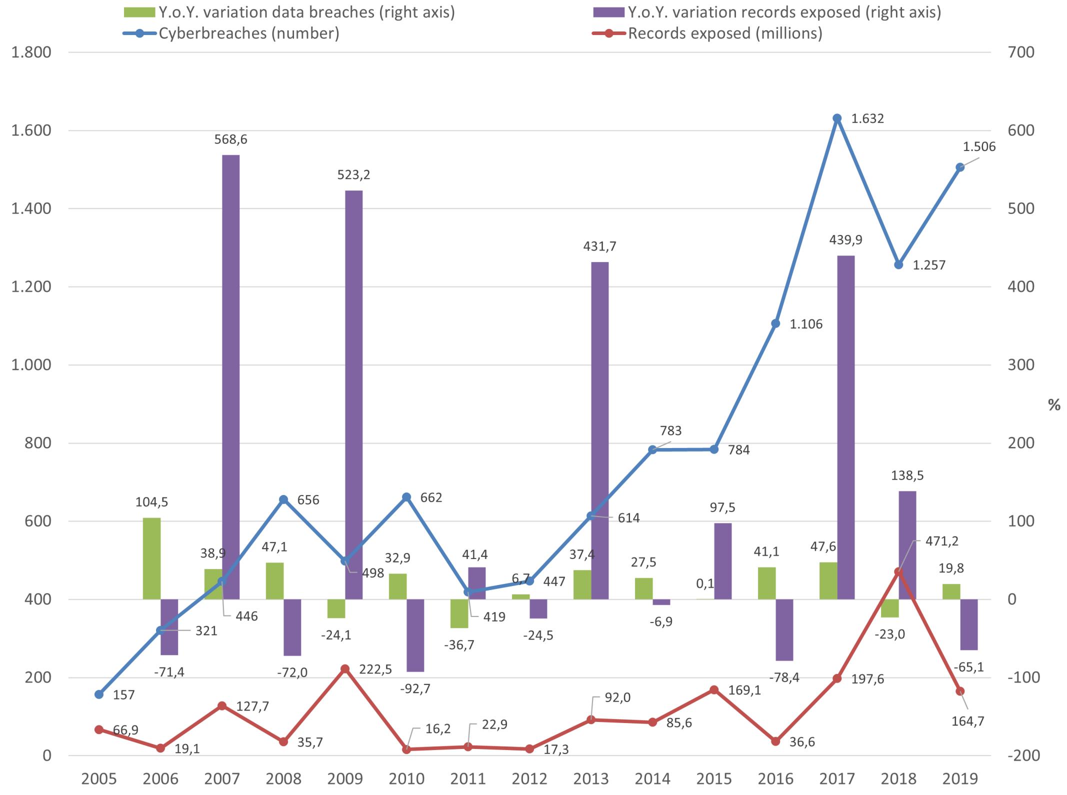
[1] See also The Economist, "Huawei is a cyber-security risk", 25 January 2020, https://www.economist.com/leaders/2020/01/25/huawei-is-a-cyber-security-risk (last accessed December 14, 2020).

[2] A data record is a set of data that could be stored, for instance, as rows in a spreadsheet.

[3] This seems to suggest that the rate of return of a single successful cyberattack increased over time, thanks probably to a rapid learning processes on the part of the attackers, or a defence system becoming rapidly obsolete, or both.

Government, 2020b) and by the widespread adoption of remote work as a result of the Covid-19 pandemic (IBM Corporation, 2020).

Figure 1: Cyberbreaches and exposed records in the US (2005-2019)



Source: Elaboration based on data from Identity Theft Resource Center.

In such a threatening ecosystem, investments in cybersecurity have become critical for firms in order to assure the integrity, confidentiality and availability of data assets and the survival of the business itself.[4] This explains why such investments have permanently entered the set of decision variables that any firm should take into account. To the best of our knowledge, there is no evidence so far for the hypothesis that the increasing costs due to cyberattacks do depend on the investments in countermeasures or on the lack thereof;[5] still, anecdotal evidence and field practitioners point out that an inadequate level of cybersecurity exposes to a higher risk of a successful attack and higher costs (Accenture, 2020). Actually, the market mechanism alone can fail to provide an efficient security level (The White House, 2003; Kopp et al., 2017). Anderson (2001) and Anderson and Moore (2006) first recognized that perverse economic incentives and market failures influence decisions on security and argued for the application of economic theories to cybersecurity issues. These important considerations stimulated the flourishing of a theoretical

[4] For instance, the safeguard of intellectual property rights from cybertheft and the appropriation of profit share from R&D activity is of vital importance for firms (Lattanzio and Ma, 2020).

[5] Roner et al. (2020) provide a first attempt to test such hypothesis.

literature on the firm decision to invest in cybersecurity. By contrast, the empirical literature is at an early stage, likely because of data scarcity (Biancotti et al., 2017; Wolff and Lehr, 2017).

The purpose of this paper is to provide a review of the theoretical contributions on firm investments in cybersecurity. In the next paragraphs, we briefly describe the four streams that characterize this literature.

Four streams of literature. The concern for cybersecurity and, more generally, security issues was boosted in the early 2000s by the September 11th terrorist attacks. Two streams of literature initially emerged that are particularly relevant to our review.

The first stream, originated by Gordon and Loeb (2002), examines firms' incentives to invest in cybersecurity using one-firm frameworks and, therefore, neglecting all forms of interdependence that can arise among firms. The predictions of this literature might not be of general applicability from a policy perspective because in most real-world situations firms conduct their business using common computer networks and/or are competitors in the product market.[6]

On this basis, a second and successful stream of literature, originated by Kunreuther and Heal (2003) and Varian (2004), investigates interdependent security - not only cybersecurity, but also, e.g., airport security, fire protection, vaccinations - using multi-firm settings. In the specific context of cybersecurity, this literature focuses on the investment decisions of firms that operate their business via a common computer network, but are not competitors in the product market. This setting can be usefully illustrated by the 2013 case of Target data breach, which involved Target Corp., one of biggest retail corporations in the US, and Fazio Mechanical Services Inc., a small company in the sector of heating, ventilation and air conditioning, also based in the US. While the two companies were apparently not competitors, they were interconnected because, as part of their services, Fazio's technicians used to connect to Target's computer network to perform remote control and maintenance of the heating system.

A few years later, a third and growing strand of literature, originated by Garcia and Horowitz (2007), shifted the focus to the cybersecurity investment choices of firms that are competitors in the product market, but run their business using non-interconnected computer systems. Amazon.com Inc. and eBay Inc. represent a good case in point for this setting as they are competitors in the e-commerce sector, but rely on different (back-end) computer systems for their business activity.

Recently, a few papers started investigating the incentive to invest in cybersecurity of firms that use a common computer network and, at the same time, are competitors in the product market. The banking sector provides a good real-world example of such a framework. Banks tend to be direct competitors and are also closely interconnected as they take part in networks that are essential for their daily business

[6] A computer network is a set of connected devices. The connection can be physical through a cable, or wireless. Connected devices share resources, like access to the Internet, printers, file servers, data and others.

operations; one can think of the SWIFT (Society for Worldwide Interbank Financial Telecommunications) network, which banks rely on to transfer funds worldwide.

Existing surveys on cybersecurity and our contribution. There exist some review papers on security in computer and communication networks (Liang and Xiao, 2013; Manshaei et al., 2013; Laszka et al., 2014; Merrick et al., 2016; Iqbal et al., 2019).[7] These surveys - written by and addressed to computer scientists - concentrate on firms that operate their business via common computer networks, but are not competitors in the product market. Game-theoretic approaches are used to study different issues, such as cyberinsurance, anonymity and privacy, vehicular network security, intrusion detection systems, and smart grid protection; only Laszka et al. (2014) have a main focus on firms' strategic decisions related to cybersecurity investments.

To the best of our knowledge, our paper is the first attempt to provide a comprehensive review of the research on the economics of cybersecurity, with a specific focus on firm(s)' investments in cybersecurity. Doing so, we complement the existing computer science contributions by reviewing all the four streams of literature previously described, that is, one-firm frameworks of cybersecurity investments and multi-firm frameworks with competing firms too.

The paper is organized as follows. Section 2 describes the dimensions we rely on to categorize the surveyed articles and presents a summary table to highlight the differences across articles according to such dimensions. Section 3 outlines a model of investment in cybersecurity that encompasses most articles on the basis of the dimensions introduced in Section 2 and provides a tool to understand the other contributions. Section 4 concludes. The appendix contains mathematical proofs of some of the results derived in Section 3.

2 A map of the literature

The vast and heterogeneous theoretical literature on investments in cybesecurity tends to abstract from the actual form and technical details of the investments in cybersecurity and to not consider the different types of attacks (e.g., denial-of-service attacks, password attacks, phishing, ransomware attacks). Moreover, the terms "cybersecurity", “IT security”, “network security”, “computer security”, and “information security” are generally used interchangeably.

To provide a comprehensive and, at the same time, reader-friendly review of this literature, we proceed in two steps. First, we identify five dimensions that crucially characterize the existing contributions and

[7] The conference papers by Roy et al. (2010) and Böhme and Schwartz (2010) are worth mentioning too.

use them to build a map of the literature. Table 1 reports the categorization of the papers according to these dimensions.

1. The dimension "investment" refers to two alternative scenarios: either the cybersecurity investment level can take any nonnegative value in the set of real numbers $\mathbb{R}$ - *continuous investment* - or it is simply a binary decision (investing/not investing) - *dichotomous investment*.

2. The dimension "interdependence" refers to whether the investment choice is analyzed in one-firm settings, using decision theory, or in multi-firm settings, using noncooperative game theory.

3. Only for papers allowing for interdependence, the dimension "welfare" indicates whether the socially efficient investment level is calculated and compared to the equilibrium level or not.

4. Only for papers allowing for interdependence, the dimension "spillovers" describes different forms of externalities related to the three multi-firm streams of literature described in the introduction.

   (i) When firms are interconnected through a common computer network, but they are not competitors in the product market, the investment by any single firm is assumed to reduce the probability of a security breach suffered by all the other firms on the network. This is referred to as *technical spillovers.*[8]

   (ii) When firms are competitors, but use non-interconnected computer systems, firms suffering a cyberattack are assumed to lose clients who shift to competitors that are not hit by any attack. This is referred to as *market spillovers.*

   (iii) When firms are both interconnected and competitors, *technical and market spillovers* are simultaneously present.

5. Only for papers considering technical spillovers, the dimension "network" refers to whether the topology of the computer network connecting the firms is exogenously assumed - *exogenous network* - or it endogenously arises as a solution to a specific optimization problem - *endogenous network.*[9]

Second, in the next section we build a model of investment in cybersecurity that encompasses most contributions in a common reference framework and helps discuss the main findings of the remaining contributions. We initially consider a one-firm setting to analyze the literature with no interdependence. We then enrich the model to allow for interdependence in the form of first technical spillovers, then

[8] Technical spillovers capture additive interdependence among firms, that is, a situation in which the overall level of the computer network security is the (possibly weighted) summation of the investments undertaken by each single firm on the network. There are only two papers, namely Varian (2004) and Grossklags et al. (2008), who, on top of additive interdependence, consider two other forms of interdependence, "weakest-link" and "best-shot", according to which the computer network security level is determined by the smallest and the largest individual investment, respectively.

[9] A (computer) network topology is a geometrical model that represents how the connections among the devices are configured.

market spillovers, and finally both types of spillovers. The investment is assumed to be continuous and, when interdependence is present, a welfare analysis is carried out to make a comparison between the equilibrium investment and the socially efficient investment, defined as the level that maximizes the sum of all firms' payoffs.[10] Finally, when technical spillovers are analyzed, the topology of the computer network connecting the firms is exogenously given.

Table 1: A taxonomy of studies on cybersecurity investments

Reference	Investment	Interdependence	Welfare	Spillover	Network
Gordon and Loeb (2002)	Continuous	No	-	-	-
Hausken (2006)	Continuous	No	-	-	-
Willemson (2006)	Continuous	No	-	-	-
Wang (2017)	Continuous	No	-	-	-
Baryshnikov (2012)	Continuous	No	-	-	-
Lelarge (2012)	Continuous	No	-	-	-
Willemson (2010)	Continuous	No	-	-	-
Gordon et al. (2003)	Dichotomous	No	-	-	-
Kunreuther and Heal (2003)	Dichotomous	Yes	No	Technical	Exogenous
Böhme (2012)	Continuous	Yes	Yes	Technical	Exogenous
Varian (2004)	Continuous	Yes	Yes	Technical	Exogenous
Grossklags et al. (2008)	Continuous	Yes	Yes	Technical	Exogenous
Riordan (2014)	Continuous	Yes	Yes	Technical	Exogenous
Lelarge and Bolot (2008)	Dichotomous	Yes	Yes	Technical	Exogenous
Lelarge (2009)	Dichotomous	Yes	Yes	Technical	Exogenous
Lelarge (2012)	Dichotomous	No/Yes**	Yes	Technical	Exogenous
Miura-Ko et al. (2008)	Continuous	Yes	No	Technical	Exogenous
Nguyen et al. (2009)	Dichotomous	Yes	No	Technical	Exogenous
Jiang et al. (2011)	Continuous	Yes	Yes	Technical	Exogenous
Acemoglu et al. (2016)	Continuous	Yes	Yes	Technical	Exogenous
Dziubiński and Goyal (2017)	Dichotomous	Yes	Yes	Technical	Exogenous
Dziubiński and Goyal (2013)	Dichotomous	Yes	No	Technical	Endogenous
Goyal and Vigier (2014)	Discrete*	Yes	No	Technical	Endogenous
Cerdeiro et al. (2017)	Dichotomous	Yes	Yes	Technical	Endogenous
Garcia and Horowitz (2007)	Dichotomous	Yes	Yes	Market	-

Continues on the next page

[10] This definition of social welfare implies that the equilibrium level is trivially equivalent to the socially efficient one in one-firm settings.

Continues from the previous page

Reference	Investment	Interdependence	Welfare	Spillover	Network
Nagurney and Nagurney (2015)	Continuous	Yes	No	Market	-
Arce (2018)	Continuous	Yes	No	Market	-
Arce (2020)	Continuous	Yes	No	Market	-
Gao and Zhong (2016)	Continuous	Yes	No	Market	-
Qian et al. (2019)	Continuous	Yes	No	Market	-
Liu et al. (2018)	Continuous	Yes	No	Market	-
Liao and Chen (2014)	Dichotomous	Yes	No	Technical & Market	Exogenous
Jianqiang et al. (2015)	Continuous	Yes	Yes	Technical & Market	Exogenous

[*] In Goyal and Vigier (2014), the cybersecurity investment level can take any nonnegative value in the set of natural numbers $\mathbb{N}$.

[**] Lelarge (2012) first considers a one-firm setting and then extends the analysis to multiple interconnected firms.

3 An encompassing model of cybersecurity investment

3.1 No interdependence

The simplest framework to study the economic trade-offs connected with investments in cybersecurity is a one-period model with (only) one decision-maker. In this model, interdependence is ruled out by assumption, hence the decision process does not depend on factors pertaining to other agents.

A risk-neutral firm decides how much to invest in security countermeasures to protect a set of information. We introduce the following notation: (i) X is the value of the firm information set, referred to as the firm revenue; (ii) $t \in [0,1]$ is the probability that a cyberattack occurs; (iii) $v \in [0,1]$ is the vulnerability of the firm information set, that is, the ex ante probability of an information set security breach, before any investment in cybersecurity is made, conditional on a cyberattack occurring; (iv) aX, $a \in [0,1]$ is the monetary loss due to a security breach.[11] We let the probability t be equal to 1. The firm invests a continuous monetary amount $I \geq 0$ to decrease the vulnerability v.[12] The ex post probability function of a security breach, once the investment I has been made, is denoted by $\pi(I,v) \in (0,v]$ and is characterized by the following three assumptions:

A1 $\pi(I,0) = 0$

A2 $\pi(0,v) = v$

[11] The value aX captures the direct and indirect losses generated by a breach and can be estimated by the value of the revenue lost as a consequence of the breach. This is why it is assumed to be proportional to X.

[12] Time is disregarded. An investment increases the security level without any time lag.

A3 π is continuously twice differentiable with respect to I and for $0 < v < 1$:

$\frac{\partial \pi(I,v)}{\partial I} < 0$, $\frac{\partial^2 \pi(I,v)}{\partial I^2} > 0$, and $\forall v \lim_{I \to \infty} \pi(I,v) = 0$

According to **A1**, if the vulnerability is zero, $v = 0$, the ex post probability stays at zero after every possible level of investment, $\pi = 0$. **A2** states that if the level of security investment is zero, $I = 0$, the ex post probability equals the vulnerability, $\pi = v$. According to **A3**, the investment reduces the ex post probability at a decreasing marginal rate (i.e., π shows decreasing marginal returns to I).

Overall, the firm decision process can be formalized by the following problem:

$$\max_{I \geq 0} R(I) - I = \{X - [\pi(I,v)]\, aX - I\} \tag{1}$$

The firm chooses the investment level I to maximize its payoff, $R(I) - I$, which is given by the firm revenue minus the expected loss due to a cyberattack, $X - [\pi(I,v)]\, aX$, net of the investment cost I. The first order condition of problem (1) is

$$-\frac{\partial \pi(I,v)}{\partial I} aX = 1 \tag{2}$$

Solving (2) by I yields the optimal investment level, denoted by I^*, at which the marginal benefit of the investment - the reduction in the expected loss due to a cyberattack - equals its marginal cost. To provide a closed-form solution to equation (2), we consider the following explicit probability function, which conforms with Assumptions **A1-A3**,

$$\pi_0(I,v) = \frac{v}{I+1} \tag{3}$$

Plugging (3) into (2) and solving by I yields

$$I^* = \sqrt{vaX} - 1 \tag{4}$$

Two interesting results characterize this optimal level of investment. First, I^* increases both with the loss incurred by the information set to be defended, aX, and with the vulnerability, v. Second, dividing I^* in (4) by the expected loss without protection, vaX, yields a maximum of 0.25 for any value of vaX; this means the optimal investment level never exceeds 25 percent of the expected loss before any investment in security is made.

The above framework can be used to illustrate the theoretical literature studying cybersecurity corporate investments in the absence of firms' interdependence. The seminal contribution by Gordon and Loeb (2002) uses a generalized version of our framework. They consider two classes of security breach explicit probability functions, which conform with Assumptions **A1-A3**,

$$\pi_1(I,v) = \frac{v}{(\alpha I+1)^{\beta}} \tag{5}$$

$$\pi_2(I,v) = v^{\alpha I+1}$$

with $\alpha > 0$ and $\beta \geq 1$.[13] The authors find two additional results compared to our simpler framework. First, they derive an inverted U-shaped relationship between the optimal investment and the vulnerability, v, when $\pi_2(I,v)$ is considered. Second, they show that the upper bound on the optimal investment rises from 25 to 36.8 percent ($\approx \frac{1}{e}$) of the expected loss without protection, when either $\pi_1(I,v)$ or $\pi_2(I,v)$ are considered. The first result did not draw much attention in the literature.[14] By contrast, the potentially practical relevance of the second result as guidance for decision-making gave rise to a debate concerning its robustness.

A first group of papers consider different classes of security breach explicit probability functions to investigate the role played by Assumptions **A1-A3** in determining the precise percentage value of the upper bound. Even though **A3** finds supporting evidence in Tanaka et al. (2005), who study 3,241 local e-government infrastructures in Japan, Hausken (2006) relaxes it and considers probability functions that also exhibit increasing, first increasing and then decreasing, or constant marginal returns to investment I. The conclusion pooling together all these different specifications is that the optimal investment is no longer bounded at 36.8 percent ($\approx \frac{1}{e}$) of the expected loss without protection. A clear intuition for this result is provided by Willemson (2006), who considers linear probability functions to further investigate the case of constant marginal returns. Since this specification implies that cyberattacks can be completely neutralized by investing enough in security, the upper bound on the optimal investment is proved to approach 100 percent. In line with these papers, Wang (2017) introduces other classes of probability functions that relax Assumption **A3** and confirms that the upper bound on the optimal investment can rise above 36.8 percent. Also Assumption **A2**, which states that a firm can be partially protected even when no investment in security is undertaken (i.e., $\pi = v \in [0,1]$ when $I = 0$), is modified in Wang (2017). The author posits the more realistic hypothesis that a firm information set is instead breached with certainty at zero security spending if a cyberattack occurs (i.e., $\pi = 1$ when $I = 0$).

A second group of papers shifts the focus from explicit to generic security breach probability functions and the mathematical conditions these generic functions must fulfill for the optimal investment to be upperly bounded. Baryshnikov (2012) and Lelarge (2012) generalize Gordon and Loeb (2002) by

[13] Note that $\pi_0(I,v)$ in (3) is a special case of $\pi_1(I,v)$ with $\alpha = \beta = 1$.

[14] The only exception is Lelarge (2012), who derives mathematical conditions that the firm payoff - as in (1) - must fulfill for the efficient investment to be monotonically non-decreasing in v. These conditions exclude inverted U-shaped relationships.

proving that if a generic probability function is non-increasing and log-convex in I, then the optimal investment is bounded by 36.8 percent ($\approx \frac{1}{e}$) of the expected loss without protection.[15] Log-convexity always implies **A3**, while **A3** does not always imply log-convexity. This explains why the papers discussed in the previous paragraph find upper bounds above 36.8 per cent; most of the explicit probability functions considered there do not fulfill **A3**, therefore failing to fulfill the more restrictive log-convexity property too.

To conclude the review of the literature with no interdependence among firms, we discuss Willemson (2010) and Gordon et al. (2003). Willemson (2010) observes that any security breach probability function should fulfill the reasonable property of being strictly increasing in v. This is indeed the case with our specification, expression (3), and the two functions considered by Gordon and Loeb (2002), expressions (5). However, the author provides a counterexample of a function that does not fulfill this property, despite complying with Assumptions **A1**-**A3**. For this reason, he suggests to extend this set of assumptions and include that $\frac{\pi(I,v)}{\partial v}$ must be strictly positive for any I. Gordon et al. (2003) offer a broader perspective on the decision to invest in cybersecurity by considering it in the light of the real options theory. This approach adds a temporal dimension to the investment problem. Unlike in the papers discussed above, the firm in Gordon et al. (2003) does not simply choose whether to invest (now), but also when to invest. This additional option is a relevant and a realistic one because cybersecurity investments are usually characterized by two aspects: (i) irreversibility, due to the fact that it is technically impossible or very costly to disinvest and free resources; (ii) enduring uncertainty about the occurrence of security breaches. The interplay of irreversibility and uncertainty can support the decision to defer the investment. For example, if a firm operates in a sector where uncertainty is high (low) because cyberattacks seldom (often) occur, the decision to defer an irreversible investment can be more (less) valuable. On this ground, Gordon et al. (2003) remark that in order for a firm to find it profitable to invest now, the net present value of the investment needs not only to be positive, but also greater than the option value associated with deferring the investment until uncertainty is reduced, as in the occurrence of a security breach.

In the next three sections, we extend our framework to allow for (different types of) interdependence among firms. In doing so, we take on board the insight from Wang (2017) and modify Assumption **A2** by letting a firm information set be completely vulnerable, $v = 1$, at zero security spending, $I = 0$. Accordingly, we rewrite the probability function (3) as

$$\pi_0(I) = \frac{1}{I+1} \tag{6}$$

[15] A function is log-convex if the logarithm of this function is convex.

and the optimal investment as

$$I^* = \sqrt{aX} - 1 \tag{7}$$

3.2 Interdependence: technical spillovers

In this section, we investigate interdependence among firms in the form of technical spillovers. We consider $N \geq 2$ symmetric and risk-neutral firms that operate their business via the same computer network, but are not competitors in the product market. Firms face the same probability $t = 1$ of suffering a cyberattack and simultaneously decide how much to invest in cybersecurity. The investment by one firm reduces the probability of a security breach suffered by this firm - this is the same (private) benefit considered in Section 3.1 - and it also contributes to reduce the probability of a security breach suffered by all the other firms within the network - this is the technical spillovers effect.

To illustrate step by step hypotheses and results of this framework, we first calculate the equilibrium investment in case of $N = 2$ symmetric risk-neutral firms that are operationally connected via a computer network. We then extend the analysis to the general case with $N \geq 2$ firms.

Two firms. Each firm $i = 1,2$ simultaneously solves the following problem:

$$\max_{I_i \geq 0} R_T\left(I_i, I_j\right) - I_i = \left(X - \frac{1}{I_i + eI_j + 1} aX - I_i\right) \tag{8}$$

Firm i payoff is denoted by $R_T\left(I_i, I_j\right) - I_i$, T being a mnemonic for technical spillovers; it is given by the revenue X, which is assumed to be constant across the firms, minus the expected monetary loss due to a cyberattack, $\frac{1}{I_i+eI_j+1}aX$, net of the investment cost I_i. The expression for the ex post probability of a security breach, $\frac{1}{I_i+eI_j+1}$, extends (6) to account for technical spillovers. In particular, parameter $e \in [0,1]$ captures the positive spillovers produced by the investment of firm $j \neq i$ on the security level enjoyed by firm i. When $e = 0$, no technical spillovers arise in that firm j's investment has no bearing on the probability that firm i suffers a loss; when $e = 1$, the technical spillovers are at their maximum in that the reduction in the probability of a security breach enjoyed by firm i thanks to firm j's investment is as big as that enjoyed by firm j itself. The first order condition of problem (8) is

$$I_i^*(I_j) = \sqrt{aX} - 1 - eI_j \tag{9}$$

and yields the best response function of firm i, that is the solution to problem (8) as a function of the investment level chosen by firm j, I_j. Relying on firms' symmetry, we can calculate the symmetric Nash equilibrium level of each firm's investment,

$$I_T^*(2) = \frac{\sqrt{aX}-1}{1+e} \tag{10}$$

Expression (10) shows that accounting for interdependence in the form of technical spillovers alters the outcome compared to the one-firm framework. The equilibrium level of investment is increasingly lower than the optimal level calculated in the one-firm case, $I^* = \sqrt{aX}-1$, as $e > 0$ rises. The reason is that the growing technical spillovers induce each firm to increasingly free ride on the other firm's investment effort. Instead, when $e = 0$, $I_T^*(2)$ turns out to be equal to $I^* = \sqrt{aX}-1$ because the absence of spillovers does not trigger any free-riding behavior.

N **firms.** The two-firm framework can be easily extended to account for $N \geq 2$ symmetric risk-neutral firms operationally connected via a computer network. The problem simultaneously solved by each firm $i = 1,...,N$ becomes

$$\max_{I_i \geq 0} R_T(I_1,...,I_N) - I_i = X - \frac{1}{I_i + e\sum_{j \neq i}^{N-1} I_j + 1} aX - I_i \tag{11}$$

The only difference between gross payoffs $R_T(I_1,...,I_N)$ and $R_T(I_i,I_j)$ lies in the expression for the ex post probability of a security breach, $\frac{1}{I_i+e\sum_{j\neq i}^{N-1} I_j+1}$, now extended to the summation of the investments chosen by all $N-1$ firms but firm i, weighted by parameter e. Computing the first order condition of problem (11) and then solving for the symmetric Nash equilibrium chosen by each firm yields

$$I_T^*(N) = \frac{\sqrt{aX}-1}{1+(N-1)e} \tag{12}$$

As in case $N = 2$, the equilibrium investment equals the one-firm optimal level $I^* = \sqrt{aX}-1$ in the absence of spillovers, $e = 0$, but it is increasingly lower as e rises because of free riding. The additional interesting result is that, for any given $e > 0$, $I_T^*(N)$ is negatively affected by N too. A computer network connecting an increasing number of firms leads thus to a decreasing per-firm investment in cybersecurity. The reason is that the free-riding problem exacerbates when each firm can enjoy technical spillovers originating from a growing number of firms within the network. In the limit, that is when $N \to \infty$, $I_T^*(N)$ approaches zero and no firm is willing to invest.

Our model can be used to provide a welfare analysis. For any given N, we compare the equilibrium investment, $I_T^*(N)$ in (12), to the socially efficient investment, defined as the level chosen by a social planner to maximize the sum of all firms' payoffs. We denote the socially efficient investment by $I_T^E(N)$

and obtain it as a solution to

$$\max_{I\geq 0} N\times\left[R_T\left(I\right)-I\right]=N\left(X-\frac{1}{I+e\left(N-1\right)I+1}aX-I\right)$$

where $N\times\left[R_T\left(I\right)-I\right]$ is the sum of firms' payoffs. We get

$$I_T^E\left(N\right)=\frac{\sqrt{\left[1+\left(N-1\right)e\right]aX}-1}{1+\left(N-1\right)e}$$

Comparing $I_T^*\left(N\right)$ to $I_T^E\left(N\right)$ reveals that the equilibrium investment is below the socially efficient level for any given $N\geq 2$ when $e>0$; firms invest too little in cybersecurity. This underinvestment normative outcome is due to the positive externality created by the technical spillovers. When any firm i decides to increase I_i to enhance security, the private marginal benefit (i.e., the increase in firm i payoff) is lower than the social marginal benefit (i.e., the increase in the sum of all firms' payoffs) because the former does not internalize the reduction in the probability of a security breach enjoyed by all the other $N-1$ firms.

We use the above framework to discuss the vast literature studying cybersecurity corporate investments when firms' interdependence takes the form of technical spillovers. The seminal contribution by Kunreuther and Heal (2003) is based on a simplified version of our framework, in which the investment level is a dichotomous, rather than a continuous, variable. To illustrate Kunreuther and Heal (2003), who begin their analysis with the case of $N=2$ firms, we therefore assume that the investment level chosen by each firm $i=1,2$ can be either 0, or an arbitrarily positive value I. Substituting $I_i=\{0,I\}$ into $R_T\left(I_i,I_j\right)-I_i$, the objective function of firm $i=1,2$ problem (8), yields the following game:

Firm 1; Firm 2	I	0
I	$R_T\left(I,I\right)-I;R_T\left(I,I\right)-I$	$R_T\left(I,0\right)-I;R_T\left(0,I\right)$
0	$R_T\left(0,I\right);R_T\left(I,0\right)-I$	$R_T\left(0,0\right);R_T\left(0,0\right)$

(13)

where

$$\begin{gathered}R_T\left(I,I\right)=X-\tfrac{1}{I+eI+1}aX\geq R_T\left(I,0\right)=X-\tfrac{1}{I+1}aX\geq\\ R_T\left(0,I\right)=X-\tfrac{1}{eI+1}aX\geq R_T\left(0,0\right)=X-aX\geq 0\end{gathered}\tag{14}$$

Kunreuther and Heal (2003) observe that the Nash equilibrium of this game prescribes investment in cybersecurity by both firms if $R_T\left(I,I\right)-I\geq R_T\left(0,I\right)$, or, equivalently

$$R_T\left(I,I\right)-R_T\left(0,I\right)\geq I\tag{15}$$

that is, the benefit due to the reduced probability of a breach, given that the other firm decides to invest, is not lower than the investment cost. By contrast, a firm operating its business via an isolated computer system has a payoff of $X - \frac{1}{I+1}aX - I$, when investing, and of $X - aX$, when not investing. These two payoffs, obtained by plugging I and 0 into $R(I)$, the objective function of problem (1) with $\pi_0(I) = \frac{1}{I+1}$, are equivalent to $R_T(I,0)$ and $R_T(0,0)$ in (14). A firm in isolation is thus willing to invest if and only if

$$R_T(I,0) - R_T(0,0) \geq I \tag{16}$$

One can easily check the left hand side of (15) is lower than that of (16) when $e > 0$,

$$R_T(I,I) - R_T(0,I) < R_T(I,0) - R_T(0,0) \tag{17}$$

that is, the investment is less effective in reducing the probability of a breach when there are technical spillovers originating from a second firm. Kunreuther and Heal (2003) conclude that in the following parametric interval

$$R_T(I,I) - R_T(0,I) \leq I < R_T(I,0) - R_T(0,0) \tag{18}$$

where (16) is fulfilled but (15) is not, the presence of a second firm in the computer network reduces the incentive to invest in cybersecurity.[16] The authors then extend the analysis to $N \geq 2$ firms and find that the condition for the Nash equilibrium to prescribe investment by all firms becomes monotonically tighter as N increases; in the limit, that is when $N \to \infty$, no firm is willing to invest Kunreuther and Heal (2003, p. 243, equation 5).

A stream of literature extends Kunreuther and Heal (2003) by considering continuous investments and providing welfare analyses. Böhme (2012) investigates two interconnected firms and explicitly distinguishes between a direct risk that each firm is hit by a cyberattack and an indirect risk of contagion from the other firm.[17] The author shows that a Nash equilibrium, if any, is characterized by underinvestment. A similar normative outcome is obtained by Varian (2004) who focuses on the case of maximum technical spillovers across firms, corresponding to $e = 1$ in our framework. Grossklags et al. (2008) extend Varian (2004) to allow for a second type of cybersecurity investments; not only self-protection investments reducing the probability that a security breach takes place, but also self-insurance investments, such as regular

[16] The original formulation of game (13) in Kunreuther and Heal (2003) is slightly different in that the two Nash equilibria when (18) holds true prescribe either investment by both firms - (I,I) - or no investment - $(0,0)$ - whereas they always prescribe investment by only one firm in our game - $(I,0)$ or $(0,I)$. This implies that condition (15) is only sufficient to have investment by both firms in Kunreuther and Heal (2003), whereas it is also necessary in our setting.

[17] In our framework, the direct and indirect risks are both embedded in the expression for the firm i ex-post probability of a security breach, $\frac{1}{I_i + e\sum_{j \neq i}^{N-1} I_j + 1}$; firm i reduces the direct risk of being attacked by increasing I_i, while it is exposed to a lower indirect risk when any other firm $j \neq i$ increases I_j.

backups on existing data, that limit the amount of the loss in case a breach occurs. While self-protection generates positive externalities in the form of technical spillovers, self-insurance does not. As a result, the authors find that the self-protection investments can be suboptimal from a welfare perspective, while the self-insurance investments are always at the socially efficient level.[18]

The analysis by Grossklags et al. (2008) makes it clear that different types of precautions against cyberattacks crucially affect the incentive to invest in cybersecurity. Some papers further investigate this aspect by considering the possibility that an investment protects not only against a direct risk of a cyberattack, as assumed by all the above contributions, but also against an indirect risk of contagion from other firms on the same network. In a two-firms framework, Riordan (2014) observes that a higher effectiveness of the protection from contagion makes less relevant the positive spillovers coming from a lower indirect risk suffered by one firm thanks to the investment of the other firm. As a result, the underinvestment issue tends to reduce. Instead, Lelarge and Bolot (2008), and Lelarge (2009, 2012) find that underinvestment may arise even if an investment cancels the risk of contagion. The intuition is that an increasing number of firms that decide to invest may reduce the direct risk that any single firm is attacked because attacks are less likely to occur against networks where viruses spread less easily. If this is the case, any single firm has less incentive to invest.

The contributions discussed so far share the following assumption: interdependence among firms is symmetric in that each firm equally affects the other firms' security.[19] This is a simplifying hypothesis in that firms can be interconnected in different ways, as remarked by Anderson and Moore (2006). In turn, different interdependences can impact differently on the dynamics of cyberconflicts and on the cybersecurity investment strategies. On this basis, a stream of literature examines situations in which firms show different degrees of influence on each other's security. Miura-Ko et al. (2008) allow any two firms in a N-firm network to change the level of reciprocal technical spillovers, with the effect that asymmetric interdependence can arise among firms on the whole network. The authors observe that any two firms can cooperate to increase the positive spillovers between them; as a result, they can invest less but enjoy the same level of security, therefore being better-off.[20] However, the reduced investment negatively affect other connected firms, which enjoy lower externalities. A similar framework is developed by Nguyen et al. (2009), who yet consider a centralized defense against cyberattacks (i.e., a central planner that de-

[18] An underinvestment issue is highlighted by Gordon et al. (2015a) too. This paper, however, uses the one-firm setting of Gordon and Loeb (2002) and modifies it to allow for a social loss stemming from a cyberattack that exceeds the private loss - aX in our framework - suffered by the firm. The source of the social loss is not formally examined but simply postulated on the basis that a computer network can allow an attacker to take control of a firm's server and then compromise all the connected firms. Relying on these theoretical considerations, Gordon et al. (2015b) discuss centralized mechanisms to offset the underinvestment tendency of the private sector.

[19] Symmetric interdependence is captured in our framework by parameter e being the same across all firms.

[20] The spirit of this twofold effect can be captured in our symmetric interdependence framework too. On one hand, $I_T^*(N)$ in (12) decreases with the technical spillovers parameter e. On the other hand, plugging $I_T^*(N)$ into the ex-post probability of a security breach, $\frac{1}{I_i+e\sum_{j\neq i}^{N-1}I_j+1}$ yields $\frac{1}{\sqrt{aX}}$, which is independent of e.

cides how much each firm on a network has to invest in cybersecurity).[21] Acemoglu et al. (2016) extend these contributions by explicitly modelling the behavior of a strategic attacker in the context of decentralized defence. The authors observe that a strategic attacker strikes a firm taking into consideration its security investment level, rather than randomly. As a consequence, any single firm has a strong incentive to increase its countermeasures in order to discourage the attack and divert it to other firms. This negative externality leads to overinvestment, which is a novel normative result in the technical spillovers literature. In a similar framework with a strategic attacker, Dziubiński and Goyal (2017) highlight the existence of the following potential source of underinvestment: firms might find it profitable to invest only if sufficiently many other firms invest as well. This can generate coordination failures, with the effect that a fully protected network can be socially efficient, but equilibria exist where firms do not invest.

The bottom line of all the above contributions is that the topology of the computer network connecting firms is exogenously given. We conclude this section by briefly reviewing a stream of literature that, instead, studies how a network topology endogenously arises as a solution to a security game between strategic defenders and attackers. Dziubiński and Goyal (2013) examine a two-stage game between a centralized defender and an attacker. In the first stage, the defender conceives the topology of the network and chooses which firms to defend with the aim of maximizing the sum of firms' payoff. In the second stage, the attacker observes the network topology and chooses which firm(s) to attack; no contagion is allowed, that is, attacks only affect the targeted firm(s). The authors show that differently dense network topologies arise in equilibrium depending on the cost incurred by the defender to protect firms. Goyal and Vigier (2014) extend Dziubiński and Goyal (2013) by introducing the possibility of contagion. The authors identify conditions under which either a star network - every firm is connected to a central one - with all defence resources allocated to the central hub, or a network with multiple hubs arise in equilibrium. Cerdeiro et al. (2017) consider, instead, decentralized defence and the three resulting externalities, previously identified in the technical spillovers literature: (i) positive externalities, like those described in our framework, leading to underinvestment; (ii) negative externalities á la Acemoglu et al. (2016), leading to overinvestment; (iii) coordination externalities á la Dziubiński and Goyal (2017) potentially leading to underinvestment. The authors study how a network topology should look like to mitigate the perverse effect of such externalities on the firms' incentive to invest.

[21] Jiang et al. (2011) consider a different form of asymmetric interdependence, based on heterogeneous amounts of potentially harmful data traffic between each pair of firms on a network. The higher these amounts, the higher the expected loss to the firms due to a potential attack, the higher the incentive to invest in cybersecurity.

3.3 Interdependence: market spillovers

In this section, we shift to interdependence among firms in the form of market spillovers. We consider $N \geq 2$ symmetric and risk-neutral firms that face the same probability $t = 1$ of suffering a cyberattack, are direct competitors in the product market, but operate their business using non-interconnected computer systems. This implies that the investment in cybersecurity, undertaken by each firm to reduce its own probability of a security breach, does not affect the level of protection enjoyed by competitors, i.e., the technical spillovers are disregarded. We model the market spillovers in two steps. (i) We let parameter X denote the market revenue, rather than that of the single firm, and be equally shared among competing firms, so that the share accruing to each firm is $\frac{X}{N}$. (ii) We assume that firms suffering a cyberattack lose their revenue shares, which are gained by competitors that are not hit.[22] With no loss of generality, we let parameter a be equal to 1, so that the entire revenue share is lost by a firm in case of an attack.

We first illustrate the case of a duopoly, when $N = 2$ symmetric risk-neutral firms are active in the product market. We then move to the general case of oligopoly with $N \geq 2$ firms.

Two firms. Each firm $i = 1,2$ simultaneously solves the following problem:

$$\max_{I_i \geq 0} R_M(I_i, I_j) - I_i = \left[\frac{X}{2} + \frac{1}{I_i + 1}\left(-\frac{X}{2}\right) + \left(1 - \frac{1}{I_i + 1}\right)\frac{1}{I_j + 1}\frac{X}{2} - I_i \right] \tag{19}$$

Firm i gross payoff is denoted by $R_M(I_i, I_j)$, M being a mnemonic for market spillovers, and consists in three terms. The first term is the market revenue, equally shared among the two competitors. The second term is given by the probability that firm i suffers a security breach following a cyberattack, $\frac{1}{I_i+1}$, times the revenue share loss, $-\frac{X}{2}$. The third term denotes the joint event where firm i does not suffer any security breach, whilst competitor $j \neq i$ does so - the probability is $\left(1 - \frac{1}{I_i+1}\right)\frac{1}{I_j+1}$ - in which case firm i gains the revenue share of firm j, $\frac{X}{2}$.

Solving problem (19) for the symmetric Nash equilibrium level of investment yields

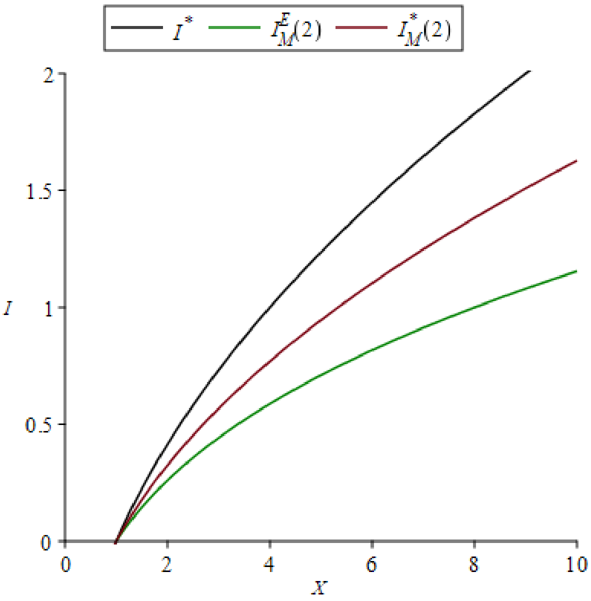
$$I_M^*(2) = \frac{X + 6H^2}{6H} - 1 \tag{20}$$

where H denotes an explicit function of the market revenue X and its expression is reported in the appendix. Figure 2 shows the plots of $I_M^*(2)$ in (20) - red curve - and I^* in (7) with $a = 1$ - black curve - as a function of X. Interestingly, $I_M^*(2)$ turns out to be lower than I^* for any given $X > 1$, meaning that the equilibrium investment shrinks when moving from monopoly to duopoly. The market spillovers yield

[22] Market spillovers find supporting evidence in Janakiraman et al. (2018), who find that consumers migrate from a compromised retailer's payment system to a safer one after a breach announcement, Jeong et al. (2019), who measure an increase in the market value of the competitors of a breached firm and Kamiya et al. (2020), who observe a decline of sales growth, ROA and cash flow of breached firms.

thus the same result as the technical spillovers. However, they operate through a different mechanism, which is not triggered by free riding and can be described as follows. A monopolistic firm that decides to increase the investment in cybersecurity is more likely not to suffer any security breach, in which case it gets the entire market revenue X. By contrast, the same additional investment undertaken by each duopolistic firm $i = 1,2$ is less effective because firm i gets the entire market revenue X only if competitor j is hit by a cyberattack, the probability of which is lower than 1 for any $I_j > 0$.

Figure 2: Equilibrium and socially efficient investments with market spillovers



We analyze the above findings from a welfare perspective too, by comparing the equilibrium investment, $I_M^*(2)$ in (20), to the socially efficient investment when $N = 2$, $I_M^E(2)$, still defined as the value chosen by a social planner to maximize the sum of the (two) firms' payoffs. We thus solve the following problem

$$\max_{I \geq 0} 2 \times [R_M(I) - I] = \left\{ 2 \left[\frac{X}{2} + \frac{1}{I+1} \left(-\frac{X}{2} \right) + \left(1 - \frac{1}{I+1} \right) \frac{1}{I+1} \frac{X}{2} - I \right] \right\} \tag{21}$$

and get

$$I_M^E(2) = \sqrt[3]{X} - 1$$

We plot this value in Figure 2 - green curve - and observe it is lower than $I_M^*(2)$ - red curve - for any given $X > 1$. The equilibrium investment is thus above the socially efficient level, i.e., firms invest too much. This overinvestment normative outcome is due to a negative externality produced by the market spillovers. If firm i decides to increase I_i to get enhanced protection, the private marginal benefit (i.e., the increase in firm i payoff) is higher than the social marginal benefit (i.e., the increase in the sum of firm i and firm j payoffs) because the former does not internalize firm j's reduced chance to gain the revenue share of firm i.

N **firms.** We extend the two-firm framework to account for $N \geq 2$ symmetric risk-neutral firms competing in the product market. The problem simultaneously solved by each firm $i = 1,...,N$ can be formulated as follows:

$$\max_{I_i \geq 0} R_M(I_1...,I_N) - I_i = \left[\frac{X}{N} + \frac{1}{I_i+1}\left(-\frac{X}{N}\right) + \left(1 - \frac{1}{I_i+1}\right)K - I_i\right] \tag{22}$$

The first and second terms within square brackets in (22) are equivalent to the respective ones in problem (19), with a generic $N \geq 2$ rather than 2. The third term is, instead, different and given by the probability that firm i does not suffer any security breach, $1 - \frac{1}{I_i+1}$, times an expression, denoted by K and whose value is reported in the appendix, describing the expected value of the gain enjoyed by firm i when it is in the position to capture the revenue share(s) of competitors suffering security breaches. We cannot derive a closed-form solution to problem (22). However, in the appendix we prove that the implicit solution, denoted by $I_M^*(N)$, is monotonically decreasing in N. The intuition is that the market spillovers make the investment in cybersecurity decreasingly effective as N rises because each firm $i = 1,...,N$ gets the entire market revenue X only if all competitors are hit by successful cyberattacks, the probability of which decreases with N. We conclude that the market spillovers' negative impact on the per-firm equilibrium investment, described above in case of duopoly, smoothly extends to the oligopoly case with $N \geq 2$ firms.

We rely on the above framework to discuss the literature studying cybersecurity corporate investments when firms' interdependence take the form of market spillovers. The seminal contribution by Garcia and Horowitz (2007) considers the investment in cybersecurity as a dichotomous variable. To illustrate their analysis, which begins with the case of $N = 2$ firms, we therefore substitute $I_i = \{0, I\}$ into $R_M(I_i, I_j) - I_i$, the objective function of firm $i = 1,2$ problem (19), and build the following game:

Firm 1; Firm 2	I	0
I	$R_M(I,I) - I; R_M(I,I) - I$	$R_M(I,0) - I; R_M(0,I)$
0	$R_M(0,I); R_M(I,0) - I$	$R_M(0,0); R_M(0,0)$

(23)

where

$$R_M(I,0) = \left(1 - \frac{1}{I+1}\right)X >$$

$$R_M(I,I) = \left(1 - \frac{1}{I+1}\right)\left[\left(1 - \frac{1}{I+1}\right)\frac{X}{2} + \frac{1}{I+1}X\right] >$$

$$R_M(0,I) = R_M(0,0) = 0$$

and, accordingly,

$$R_M(I,I) - R_M(0,I) < R_M(I,0) - R_M(0,0)$$

This inequality states that the investment is less effective in enhancing the payoff of a firm when moving from monopoly to duopoly and it is equivalent to inequality (17), derived by Kunreuther and Heal (2003). This explains why the two papers come to the same conclusion; when

$$R_M(I,I) - R_M(0,I) < I \leq R_M(I,0) - R_M(0,0)$$

a firm that is willing to invest in cybersecurity in a monopoly setting, it may not be willing anymore under duopoly. Garcia and Horowitz (2007) then generalize the analysis to the case of $N \geq 2$ firms and find that the condition under which all N firms invest at equilibrium becomes increasingly restrictive as N rises (Garcia and Horowitz, 2007, p.43, equation 2). The authors also provide a welfare analysis by comparing the equilibrium investment chosen by firms in the duopoly case to the socially efficient level. Relying on game (23), the authors remark that the private benefit enjoyed by each firm $i = 1,2$ when it decides to invest, given that firm $j \neq i$ invests as well, amounts to

$$R_M(I,I) - R_M(0,I) \tag{24}$$

By contrast, the social benefit, defined as the increase in the sum of firms' payoffs when firm i decides to invest, given that firm $j \neq i$ invests as well, is lower and amounts to

$$[R_M(I,I) - R_M(0,I)] - [R_M(I,0) - R_M(I,I)] \tag{25}$$

The second term within square brackets denotes the expected loss suffered by firm j because of the reduced chance to gain the revenue share of firm i. Overall, Garcia and Horowitz (2007) conclude that overinvestment in cybersecurity occurs when the investment cost I is larger than the social benefit (25) but lower than the private benefit (24) because both firms decide to invest at equilibrium even if this is not socially efficient.[23]

The stream of literature originated from Garcia and Horowitz (2007) extends the original contribution by modeling explicitly the behavior of the demand side of the market. The common aim of these papers is to provide a microfoundation for the consumers' choice of switching from a firm suffering a security breach to a safer competitor. By contrast, no formal welfare analyses are provided.

[23] The authors extend then the notion of social welfare to exogenously include consumer welfare. They observe that the social benefit from the investment rises above the private benefit when the consumer welfare is sufficiently high, in which case underinvestment arises (Garcia and Horowitz, 2007, p.48, equation 14).

Nagurney and Nagurney (2015) consider a competitive market with $N \geq 2$ firms and consumers who value cybersecurity. Consumers observe the average cybersecurity level of the market, but not the individual firm level (i.e., there is information asymmetry). The authors show that firms have a decreasing incentive to invest in cybersecurity as N rises, because asymmetric information increasingly prevents consumers from distinguishing firms that invest enough from those not investing adequately. In the event of a cyberattack, the less protected firms become apparent and the surviving competitors gain market shares. The role of security-aware consumers is examined also by Arce (2018) in a duopoly market. The author shows that the market share of each firm is positively affected by the own investment in cybersecurity, but negatively by the investment of the competitor. Arce (2020) extends his previous model by assuming positive costs for consumers that decide to switch to the competitor. The author proves that the lower the switching costs, the higher is the investment in security needed for a firm to retain its customers. The effect of switching customers on firms' incentive to invest is investigated also by Gao and Zhong (2016) in a duopoly market. The authors observe that as the share of switching consumers over the total number of consumers rises, firms would suffer a higher reduction in demand after a cyberattack and therefore feel pressure to improve the protection of their information assets. Each duopolist's incentive to invest hinges on two goals; not only to retain its customer base, but also to subtract switching consumers from the competitor. A similar result is derived by Qian et al. (2019). They consider a second type of consumer in addition to switching consumers, namely loyal consumers who are less sensitive to cybersecurity issues and never switch to competitors. The authors show that a greater loyal consumer base reduces the competition among firms to attract switchers and therefore the incentive to invest.

The papers reviewed so far consider firms competing in the same market by supplying substitute products. Liu et al. (2018) consider the different perspective of two firms selling complementary products. When one firm is hit by a cyberattack, also the other firm suffers a negative shock to demand because consumers cannot substitute one product for another. The authors find that a higher degree of complementarity between products enhances the positive impact of a security investment by one firm on the revenues of the second firm, which, in turn, has a stronger incentive to invest.

3.4 Interdependence: technical and market spillovers

In this section, we assume that the interdependence among firms takes the form of both technical and market spillovers. This amounts to considering firms that operate their business via a common computer network and, at the same time, are competitors in the product market.

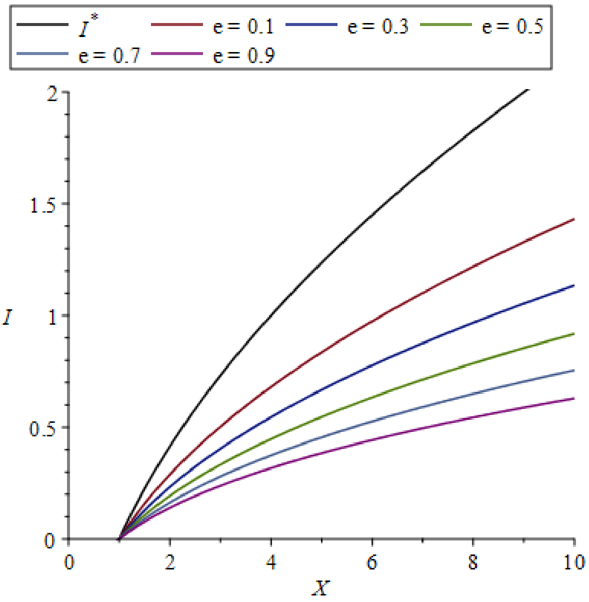
We restrict our attention to the case of $N = 2$ symmetric and risk-neutral firms that face the same probability $t = 1$ of suffering a cyberattack. Each firm $i = 1,2$ simultaneously solves the following problem:

$$\max_{I_i \geq 0} R_{TM}\left(I_i, I_j\right) - I_i = \left[\frac{X}{2} + \frac{1}{I_i + eI_j + 1}\left(-\frac{X}{2}\right) + \left(1 - \frac{1}{I_i + eI_j + 1}\right)\frac{1}{I_j + eI_i + 1}\frac{X}{2} - I_i\right] \tag{26}$$

The gross payoff $R_{TM}\left(I_i, I_j\right)$ is obtained by combining $R_T\left(I_i, I_j\right)$ in (8) with $a = 1$, when only the technical spillovers are considered, with $R_M\left(I_i, I_j\right)$ in (19), when only the market spillovers are present.

We solve problem (26) for the symmetric Nash equilibrium level of investment, denoted as $I_{TM}^*(2)$. Since the closed-form solution has a complicated expression, we resort to a graphical representation for different values of e. Figure 3 plots $I_{TM}^*(2)$ for $e = \{0.1, 0.3, 0.5, 0.7, 0.9\}$ - colored curves - and I^* in (7) with $a = 1$ - black curve - as a function of X.

Figure 3: Equilibrium investments with technical and market spillovers



All colored curves representing $I_{TM}^*(2)$ turn out to be lower than I^* for any given $X > 1$, meaning that the equilibrium investment in cybersecurity shrinks when N rises from 1 to 2, for any e. This result comes as no surprise. In Section 3.2, we show that the free-riding incentive triggered by the technical spillovers reduces a firm equilibrium investment when a second firm enters the computer network. In Section 3.3, we demonstrate that the market spillovers have a negative effect as well, because the probability that a firm gets the entire market revenue X decreases when moving from monopoly to duopoly. When both types of spillovers are accounted for, these two negative effects add up and explain the result in Figure 3. The graphical analysis also confirms that a higher technical spillovers parameter e negatively affects $I_{TM}^*(2)$ because of a growing free-riding incentive.

When the two different spillovers are simultaneously accounted for, interesting insights can be drawn from a welfare perspective because the technical spillovers alone determine underinvestment, whereas the market spillovers alone lead to the opposite result of overinvestment. It is, accordingly, worth checking under which conditions underinvestment or overinvestment prevails. To this aim, we first calculate the socially efficient investment in the usual way, i.e., as the value chosen by a social planner to maximize the sum of the two firms' payoffs,

$$\max_{I \geq 0} 2 \times [R_{TM}(I) - I] = \left\{ 2 \left[\frac{X}{2} + \frac{1}{I + eI + 1} \left(-\frac{X}{2} \right) + \left(1 - \frac{1}{I + eI + 1} \right) \frac{1}{I + eI + 1} \frac{X}{2} - I \right] \right\}.$$

Then, we compare this socially efficient level, denoted by $I^E_{TM}(2)$, to the equilibrium one, $I^*_{TM}(2)$, for any given $e = \{0.1, 0.3, 0.5, 0.7, 0.9\}$. We resort to a graphical representation, which is reported in the appendix (Figure A.2). Overinvestment, $I^*_{TM}(2) > I^E_{TM}(2)$, tends to arise at relatively low values of e. Instead, higher values of e leads to the opposite outcome of underinvestment, $I^*_{TM}(2) < I^E_{TM}(2)$. The intuition is that the market spillovers are largely prevalent when e is low. This yields the negative externality described in Section 3.3, which, in turn, makes the social benefit of the investment lower than the private benefit and determines overinvestment. As e rises, the positive externality related to the technical spillovers gets increasingly high and eventually prevails over the negative one produced by the market spillovers. As a result, the social benefit becomes higher than the private benefit and underinvestment arises.

To the best of our knowledge, the only two papers that so far study cybersecurity corporate investments when firms' interdependence take the form of both technical and market spillovers are Liao and Chen (2014) and Jianqiang et al. (2015).[24]

Liao and Chen (2014) consider $N \geq 2$ firms that can undertake a dichotomous investment in cybersecurity. Firms are symmetrically interdependent in the sense specified in Section 3.2 (i.e., each firm equally affects the other firms' security through the technical spillovers). The authors do not derive the Nash equilibrium level of the investment; rather, they examine the problem of a firm that decides to invest in cybersecurity, denote as W the resulting increase in its expected gross payoff, and ask the following question: how is W affected by the number $m \leq N-1$ of competitors that decide to invest as well? Using the notation of our framework, this question can be answered by studying the sign of the cross derivative

$$\frac{\partial^2 R_{TM}(I_i, I_j)}{\partial I_i \partial I_j}. \tag{27}$$

[24] In the context of the cyber risk information sharing literature, Böhme (2016) discusses a framework that includes both technical spillovers and market spillovers in the form of firm reputation losses when shared breach information becomes public.

In fact: (i) $R_{TM}(I_i, I_j)$ is firm i expected gross payoff; (ii) the derivative of this value with respect to I_i is the continuous counterpart of W; (iii) a variation of the (continuous) investment level undertaken by competitor j, I_j , can play the same role as the number m of competitors that undertake a (dichotomous) investment in Liao and Chen (2014). We show in the appendix that the sign of (27) is always negative in our framework, indicating that the investment levels are strategic substitutes. Liao and Chen (2014) find instead that W can be either positively or negatively affected by m. The positive relation arises when the investment in cybersecurity is particularly effective, in that the ex post proportion of firms that did not suffer any security breach after investing turns out to be higher than the ex ante probability that any single investing firm suffers no breach. In this case, the authors conclude that a firm's incentive to invest in cybersecurity is enhanced by competitors that undertake the same investment. The opposite prediction applies when, alternatively, the ex post proportion is lower than the ex ante probability.

Jianqiang et al. (2015) consider two symmetrically interdependent firms that can undertake a continuous investment and model market spillovers as an additional loss borne by any firm when this firm suffers a cyberattack, but the competitor does not. The authors calculate the Nash equilibrium level of the investment and find the following normative results: firms overinvest when market spillovers are relatively high and underinvest in the opposite scenario.

4 Conclusions

Cybersecurity has become relevant for firms aiming to protect their business from a growing number of cyber threats. Since the decision to invest in cybersecurity is influenced by economic factors, such as perverse incentives and market failures, theories and methods of economics have been increasingly applied to the study of this topic.

In this paper, we have reviewed the theoretical literature on the economics of investments in cybersecurity. We have provided a taxonomy of the studies along five characterizing dimensions and we have formalized an encompassing model to illustrate and discuss the main literature findings. We have distinguished the works that study the investment problem of an isolated firm from those that consider, instead, interconnected firms, whose interdependent cybersecurity decisions can be affected by technical spillovers, market spillovers, or both.

First, we have highlighted the two, positive and normative, basic results of the technical spillovers literature. (i) An increasing number of firms on a computer network yields a lower per-firm equilibrium investment because of free riding. (ii) This equilibrium investment is below the socially efficient level because of the positive externality created by technical spillovers. We have then considered the contributions that extend these results by examining different types of precautions against cyberattacks, asymmetric interdependencies among firms on the computer network, and endogenous network topologies.

Second, we have reviewed the market spillovers literature. We have described the positive result that the per-firm equilibrium investment is negatively affected by the number of competitors in the product market, and the normative result of overinvestment due to the negative externality brought about by this type of spillovers. We have then surveyed the articles that provide different microfoundations for the market spillovers mechanism.

Finally, we have considered the articles allowing for both types of spillovers. We have emphasized that the positive results due to technical and market spillovers add up, implying that the per-firm equilibrium investment decreases as the number of competitors using a common computer network increases. By contrast, the socially efficient outcome has been shown to be either underinvestment or overinvestment, depending on which spillovers prevail.

While the effects of technical spillovers have been extensively investigated, making this stream of theoretical literature relatively mature - except for the studies of endogenous network formation - our survey suggests promising avenues for future research.

Further interest in the market spillovers literature can be stimulated by the fact that consumers are increasingly concerned over data security and privacy (Cisco, 2020). Since most existing contributions lack a welfare analysis, the gap could be filled by explicitly modelling competition among firms through different oligopoly frameworks, such as Cournot or Bertrand, that endogenously incorporate consumer welfare. Doing so, conditions on the demand and the supply functions could be identified that affect the gap between the equilibrium investment in cybersecurity and the socially efficient investment, defined as the level that maximizes the total welfare.

Moreover, the analysis of the joint effects of technical and market spillovers is still at an early stage, partly because it requires complicated models, but potentially relevant to economic research since competitive firms increasingly rely on common computer networks to operate their businesses. For instance, mobile network operators frequently share their infrastructure to economize on the costs of upgrading the network when a new technology standard is introduced, as in the case of 5G standard (BEREC, 2018).

Finally, data on cybersecurity are becoming increasingly available from different sources, such as the Cyber Security Breaches Survey (UK Government), the Breaking Trust database (Atlantic Council) or the Chronology of Data Breaches (Privacy Rights Clearinghouse). This provides empirical economists with the opportunity to examine various issues (e.g., cyber risk, cyberinsurance, and costs of cyberbreaches) in greater detail than previously possible.

A Appendix

Expression H in (20). H is given by the following explicit function of X,

$$H = \sqrt[3]{\sqrt{\frac{X^2(27-2X)}{432}} - \frac{X}{4}}.$$

Expression K in (22). The expected gain of firm i when it does not suffer any breach can be formalized by a Poisson binomial probability distribution defined as:

$$K = \sum_{A \subseteq F_k \setminus i} \frac{X}{N} \frac{|A|}{N-|A|} \prod_{j \in A} \left(\frac{1}{I_j+1} \right) \prod_{z \in A^c} \left(1 - \frac{1}{I_z+1} \right)$$

Where:

A	Set of firms that suffer a cyberattack.
A^c	Set of firms that do not suffer a cyberattack (complement of A).
$\lvert A \rvert$	Number of firms that suffer a cyberattack.
F_k	Set of $(N-1)$ firms in the market (excluding firm i).

Relation between the implicit equilibrium solution $I_M^*(N)$ to problem (22) and N. The first order condition of (22) for a symmetric Nash equilibrium is given by:

$$\frac{X\left[1-(I+1)^{-N}\right]}{NI(I+1)} - 1 = 0 \tag{28}$$

Applying the implicit function theorem, we get the implicit derivative:

$$\frac{\partial I_M^*(N)}{\partial N} = \frac{Xln(I+1) - I(I+1)^{N+1}}{2NI(I+1)^{N+1} + N(I+1)^{N+1} - XN} \tag{29}$$

If $X < \frac{I}{ln(I+1)}(I+1)^{(N+1)}$, then the above implicit derivative is negative (i.e. the equilibrium investment decreases as the number of firms increases); if $(2I+1)(I+1)^{(N+1)} > X > \frac{I}{ln(I+1)}(I+1)^{(N+1)}$, then the implicit derivative is positive (i.e. the equilibrium investment increases as the number of firms increases). We can exclude the latter case with the help of numerical simulations of the first order condition (28) for $X \in \{2,3,4,5,6,7,8,9,10\}$ and $N \in \{2,3,4,5,6,7,8,9,10\}$. The outcome is reported in Figure A.1 and shows that $I_M^*(N)$ is decreasing in N for any given X.

Welfare analysis with technical and market spillovers. Figure A.2 reports the equilibrium investment levels - red curves, solutions to problem (26) - and the socially efficient levels - blue curves - for any given values of $e = \{0.1, 0.3, 0.5, 0.7, 0.9\}$.

Checking the sign of (27). We calculate $\frac{\partial^2 R_{TM}\left(I_i,I_j\right)}{\partial I_i \partial I_j}$ and then impose symmetry by letting $I_i = I_j = I$. We end up with

$$-\frac{X}{2}\frac{2I+4e+e^2+10eI+10e^2I+2e^3I+I^2+6eI^2+10e^2I^2+6e^3I^2+e^4I^2+1}{\left(2I+2eI+I^2+2eI^2+e^2I^2+1\right)^3}$$

which is apparently negative.

Figure A.1: Relation between $I_M^*(N)$ and N

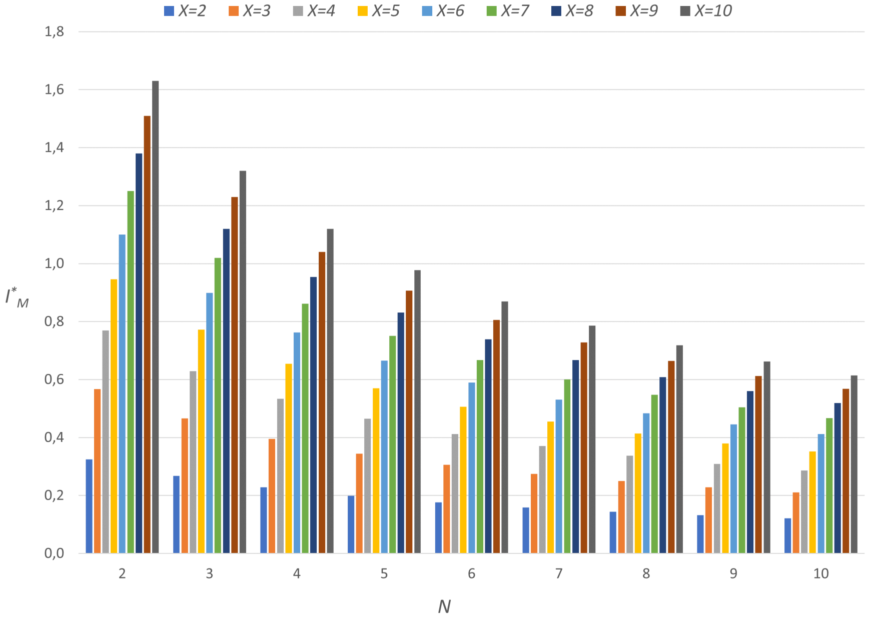
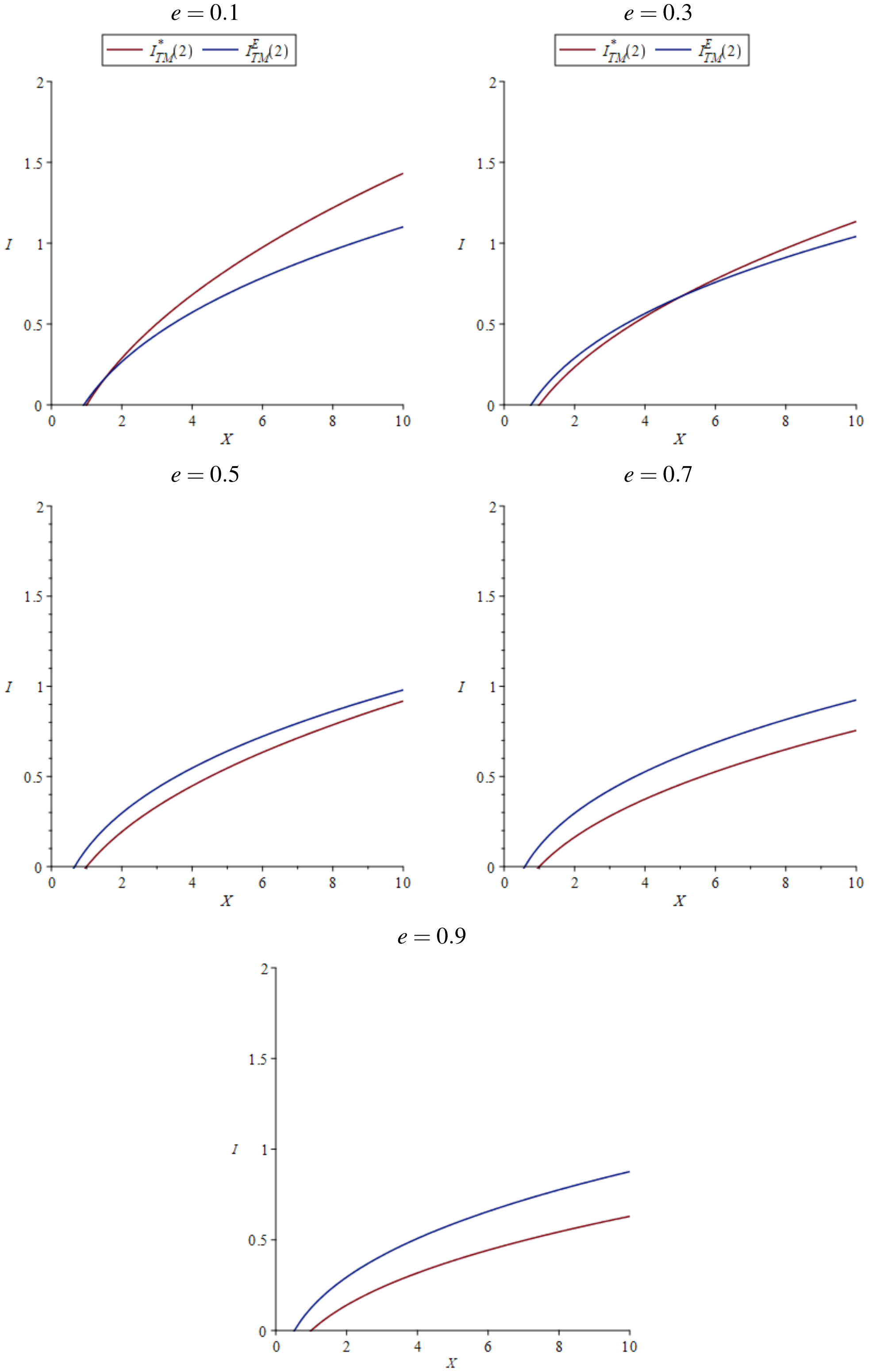


Figure A.2: Equilibrium and socially efficient investments level with technical and market spillovers



$e = 0.1$

$e = 0.3$

$e = 0.5$

$e = 0.7$

$e = 0.9$

References

Accenture (2020). Innovate for Cyber Resilience. https://www.accenture.com/_acnmedia/PDF-116/Accenture-Cybersecurity-Report-2020.pdf.

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

Amir, E., S. Levi, and T. Livne (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies 23*(3), 1177–1206.

Anderson, R. and T. Moore (2006). The Economics of Information Security. *Science 314*(5799), 610–613.

Anderson, R. J. (2001). Why Information Security is Hard – An Economic Perspective. In *Proceedings of the 17th Annual Computer Security Applications Conference*, pp. 358–365.

Arce, D. G. (2018). Malware and market share. *Journal of Cybersecurity 4*(1).

Arce, D. G. (2020). Cybersecurity and platform competition in the cloud. *Computers & Security 93*, 101774.

Baryshnikov, Y. (2012). IT security investment and Gordon-Loeb's 1/e rule. *Proceedings of the Workshop on the Economics of Information Security (WEIS)*.

BEREC - Body of European Regulators for Electronic Communications (2018). Report on infrastructure sharing. https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/8164-berec-report-on-infrastructure-sharing.

Biancotti, C. and R. Cristadoro (2018). The machine stops: The price of cyber (in)security. https://voxeu.org/article/price-cyber-insecurity. Accessed: 02/10/2019.

Biancotti, C., R. Cristadoro, S. Di Giuliomaria, A. Fazio, and G. Partipilo (2017). Cyber attacks: An economic policy challenge. https://voxeu.org/article/cyber-attacks-economic-policy-challenge. Accessed: 02/10/2019.

Böhme, R. (2012). Security audits revisited. *International Conference on Financial Cryptography and Data Security*, 129–147.

Böhme, R. (2016). Back to the Roots: Information Sharing Economics and What We Can Learn for Security. *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, 1–2.

Böhme, R. and G. Schwartz (2010). Modeling Cyber-Insurance: Towards A Unifying Framework. *Proceedings of the Workshop on the Economics of Information Security (WEIS)*.

Center for Strategic and International Studies-McAfee (2018). The Economic Impact of Cybercrime: No Slowing Down. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf.

Cerdeiro, D. A., M. Dziubiński, and S. Goyal (2017). Individual security, contagion, and network design. *Journal of Economic Theory 170*, 182–226.

Cisco (2020). Consumer Privacy Survey - Protecting Data Privacy to Maintain Digital Trust. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cybersecurity-series-2020-cps.pdf?CCID=cc000742.

Comino, S. and F. M. Manenti (2014). *Industrial Organization of High-Technology Markets: The Internet and Information Technology*. Edward Elgar publishing.

Dziubiński, M. and S. Goyal (2013). Network design and defence. *Games and Economic Behavior 79*, 30–43.

Dziubiński, M. and S. Goyal (2017). How do you defend a network? *Theoretical Economics 12*(1), 331–376.

Gao, X. and W. Zhong (2016). Economic incentives in security information sharing: the effects of market structures. *Information Technology and Management 17*(4), 361–377.

Garcia, A. and B. Horowitz (2007). The potential for underinvestment in internet security: implications for regulatory policy. *Journal of Regulatory Economics 31*(1), 37–55.

Gordon, L. A. and M. P. Loeb (2002). The economics of information security investment. *ACM (Association for Computing Machinery) Transactions on Information and System Security 5*(4), 438–457.

Gordon, L. A., M. P. Loeb, and W. Lucyshyn (2003). Information Security Expenditures and Real Options: A wait-and-see approach. *Computer Security Journal 19*(2).

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and L. Zhou (2015a). Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security 06*(01), 24–30.

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and L. Zhou (2015b). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity 1*(1), 3–17.

Goyal, S. and A. Vigier (2014). Attack, Defence, and Contagion in Networks. *The Review of Economic Studies 81*(4), 1518–1542.

Grossklags, J., N. Christin, and J. Chuang (2008). Secure or insure? A game-theoretic analysis of information security games. *Proceedings of the 17th internaltional conference on World Wide Web*, 209–2018.

Hausken, K. (2006). Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers 8*(5), 338–349.

IBM Corporation (2020). Cost of a Data Breach Report. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf.

Iqbal, A., M. Guo, L. Gunn, M. A. Babar, and D. Abbott (2019). Game theoretical modelling of network/cyber security. *IEEE Access 7*, 154167–154179.

Janakiraman, R., J. H. Lim, and R. Rishika (2018). The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer. *Journal of Marketing 82*, 85–105.

Jeong, C. Y., S.-Y. T. Lee, and J.-H. Lim (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management 56*, 681–695.

Jiang, L., V. Anantharam, and J. Walrand (2011). How Bad Are Selfish Investments in Network Security? *IEEE/ACM Transactions on Networking 19*(2), 549–560.

Jianqiang, G., M. Shue, and Z. Weijun (2015). Analyzing information security investment in networked supply chains. *2015 International Conference on Logistics, Informatics and Service Sciences (LISS)*, 1–5.

Kamiya, S., J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz (2020). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics (In press)*.

Kopp, E., L. Kaffenberger, and C. Wilson (2017). Cyber Risk, Market Failures, and Financial Stability. *IMF Working Papers 17*(185), 1.

Kunreuther, H. and G. Heal (2003). Interdependent Security. *Journal of Risk and Uncertainty 26*(2-3), 231–249.

Laszka, A., M. Felegyhazi, and L. Buttyán (2014). A Survey of Interdependent Security Games. *ACM Computing Surveys 47*(2), 23:1–23:38.

Lattanzio, G. and Y. Ma (2020). Corporate Innovation in the Cyber Age. *SSRN Electronic Journal*.

Lelarge, M. (2009). Economics of malware: Epidemic risks model, network externalities and incentives. *47th annual Allerton Conference on Communication, Control, and Computing*, 1353–1360.

Lelarge, M. (2012). Coordination in Network Security Games: A Monotone Comparative Statics Approach. *IEEE Journal on Selected Areas in Communications 30*(11), 2210–2219.

Lelarge, M. and J. Bolot (2008). Network Externalities and the Deployment of Security Features and Protocols in the Internet. *ACM SIGMETRICS Prformance Evaluation Review 36*(1), 37–48.

Liang, X. and Y. Xiao (2013). Game Theory for Network Security. *IEEE Communications surveys & Tutorials 15*(1).

Liao, C.-H. and C.-W. Chen (2014). Network externality and incentive to invest in network security. *Economic Modelling 36*, 398–404.

Liu, X., X. Qian, J. Pei, and P. M. Pardalos (2018). Security investment and information sharing in the market of complementary firms: impact of complementarity degree and industry size. *Journal of Global Optimization 70*(2), 413–436.

Manshaei, M. H., Q. Zhu, T. Alpcan, T. Bacşar, and J.-P. Hubaux (2013). Game theory meets network security and privacy. *ACM Computing Surveys 45*(3), 1–39.

Merrick, K., M. Hardhienata, K. Shafi, and J. Hu (2016). A Survey of Game Theoretic Approaches to Modelling Decision-Making in Information Warfare Scenarios. *Future Internet 8*(3), 34.

Microsoft Corporation (2016). Microsoft Advanced Threat Analytics Datasheet 2016. https://download.microsoft.com/download/C/F/6/CF62335F-C46B-4D84-B0C9-363A89B0C5E6/Microsoft_advanced_threat_analytics_datasheet.pdf.

Miura-Ko, A. R., B. Yolken, N. Bambos, and J. Mitchell (2008). Security investment games of interdependent organizations. *46th Annual Allerton Conference on Communication, Control, and Computing*, 252–260.

Nagurney, A. and L. S. Nagurney (2015). A Game Theory Model of Cybersecurity Investments with Information Asymmetry. *Netnomics 16*(1-2), 127–148.

Nguyen, K. C., T. Alpcan, and T. Basar (2009). Stochastic games for security in networks with interdependent nodes. *2009 International Conference on Game Theory for Networks*, 679–703.

Paulsen, C. (2016). Cybersecuring Small Businesses. *Computer 49*(8), 92–97.

Ponemon Institute (2019). 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses. https://www.keepersecurity.com/en_GB/ponemon2019.html.

Qian, X., J. Pei, X. Liu, M. Zhou, and P. M. Pardalos (2019). Information security decisions for two firms in a market with different types of customers. *Journal of Combinatorial Optimization 38*(4), 1263–1285.

Riordan, M. H. (2014). Security in partnerships. Working Paper.

Roner, C., C. Di Caterina, and D. Ferrari (2020). Exponential Tilting for Zero-inflated Interval Regression with Applications to Cybersecurity Survey Data (*mimeo*).

Roy, S., C. Ellis, S. Shiva, D. Dasgupta, v. Shandilya, and Q. Wu (2010). A Survey of Game Theory as Applied to Network Security. *Proceedings of the 43rd Hawaii International Conference on System Sciences*, 1–10.

Tanaka, H., K. Matsuura, and O. Sudoh (2005). Vulnerability and information security investment: An empirical analysis of e-local government in Japan. *Journal of Accounting and Public Policy 24*(1), 37–59.

The White House (2003). The National Strategy to Secure Cyberspace. https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf.

Tirole, J. (2017). *Economics for the Common Good*. Princeton University Press.

UK Government - Dept. for Digital, Culture, Media and Sport (2020). Cyber Security Breaches Survey 2020. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020.

UK Government - Huawei Cyber Security Evaluation Centre Oversight Board (2020). Annual Report. https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2020.

Varian, H. R. (2004). System reliability and free riding. In J. J. Camp and S. Lewis (Eds.), *Economics of information security*, pp. 1–16. Springer.

Wang, S. (2017). Optimal Level and Allocation of Cybersecurity Spending: Model and Formula. *SSRN Electronic Journal*.

Willemson, J. (2006). On the Gordon and Loeb Model for Information Security Investment. *Proceedings of the Workshop on the Economics of Information Security (WEIS)*.

Willemson, J. (2010). Extending the Gordon and Loeb Model for Information Security Investment. *2010 International Conference on Availability, Reliability and Security. IEEE*, 258–261.

Wolff, J. and W. Lehr (2017). Degrees of Ignorance About the Costs of Data Breaches: What Policy-makers Can and Can't Do About the Lack of Good Empirical Data. *SSRN Electronic Journal*.