TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Annika Lentso IVCM221934

Optimal Cybersecurity Investment of an Interconnected Risk-Neutral Firm

Master's Thesis

Supervisor: Adrian Venables
PhD
Co-Supervisor: Jaan Masso
PhD
(University of Tartu)

Tallinn 2025

Author’s Declaration of Originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Annika Lentso

18.05.2025

Abstract

This thesis explores the optimal level of cybersecurity investment for risk-neutral firms operating in an interconnected environment. Building on the foundational Gordon-Loeb model, the study extends the framework to include interdependence between two firms through additive and multiplicative interdependences. It introduces a game-theoretic approach under perfect and imperfect information conditions, incorporating learning dynamics to reflect real-world decision-making processes where firms update their expectations over time.

The results highlight that in additive interdependence settings, firms tend to underinvest due to strategic substitution and free-riding incentives. Introducing learning slows convergence toward equilibrium but does not eliminate the underinvestment problem. By contrast, when cybersecurity outcomes depend multiplicatively on both firms' efforts, investment decisions become strategic complements – eliminating free-riding and encouraging joint protection across the supply chain.

The thesis concludes that effective cybersecurity investment in interconnected systems requires institutional coordination, contractual enforcement, or policy interventions. These findings contribute to the theoretical development of cybersecurity economics and offer practical implications for designing regulatory and incentive frameworks that enhance collective cybersecurity resilience.

The thesis is written in English and is 55 pages long, including 4 chapters, 4 figures and 1 table.

Annotatsioon

Optimaalsed küberkaitse investeeringud ühendatud riskineutraalses ettevõttes

Käesolev magistritöö käsitleb riskineutraalsete ettevõtete küberkaitseinvesteeringute otsustusprotsessi olukorras, kus ettevõtete infosüsteemid on omavahel ühendatud ning nad tegutsevad ebakindlates tingimustes. Analüüsi aluseks on Gordon-Loebi mudel. Seda mudelit töös laiendatakse lisades tarneahela sidususe, ebatäieliku informatsiooni ja õppimisdünaamika. Töös käsitletud mudel hõlmab kahte ettevõtet ning keskendutakse nende ettevõtete vahelisele strateegilise käitumise modelleerimisele kasutades mänguteoorias tuntud Cournot oligopoli mudelit. Kui varasemad uurimused käsitlevad mängu osapooltena pigem kaitsjat ja ründajat, siis siinses töös vaadeldakse mängu kahe tarneahelas oleva ettevõtte vahel. Ka on varasemad uuringud lisanud seotuse mudelisse, kuid pigem tõenäosuste näol ründe tõenäosuse funktsioonis, siis selles töös omavaheline seotus lisatud kui partnerettevõtte investeeringud koos seotuse koefitsiendiga.

Esimene mudel, mida analüüsitakse, käsitleb aditiivset seotust ehk ühe ettevõtte investeeringutele lisandub teise oma korrutatuna seotuse koefitsiendiga. Optimaalsed investeeringuid ettevõttes mõjutab seega ettevõtte turbeparameetritele lisaks ka partnerettevõtte investeeringud. Selle mudeli peamine tulemus viitab sellele, et ettevõtted püüavad küberkaitseinvesteeringu kulu jätta teisele ettevõttele ehk nö jänest-sõitja probleem (*free rider probleem*, inglise keeles). Lisades mudelisse ebatäieliku informatsiooni ja õppimise, s.o ettevõtte arvab partneri investeeringu suurust ühel perioodil ja teisel perioodil korrigeerib arvamust olemasoleva informatsiooni põhjal, näitavad tulemused, et ettevõtted kipuvad investeerima vähem kui on optimaalne. Selline mudeli püstitus ei eelda lepingute olemasolu ega seadustest tulenevat kohustust küberkaitsesse investeerida ning nende puudumine kahandab kasumlikkust maksimeeriva ettevõtte motivatsiooni ise investeerida. Selle puuduse eemaldamiseks loodi multiplikatiivse seotusega mudel: selles mudelis sõltub küberturvalisus mõlema ettevõtte panusest. Ehk kui üks ettevõte otsustab mitte investeerida, siis teise ettevõte panus ei ole turbe seisukoht tähtis – tarneahela küberkaitse on siiski ebapiisav. Sellega võetakse arvesse ka seda, et ühe ettevõtte turvanõrkust ära kasutades, võib lekkida ka teise ettevõtte info. Teiste sõnadega, kogu tarneahela küberturvalisus sõltub mõlema ettevõtte panusest ning ühe osapoole panus võib kasvatada teise motivatsiooni küberturbesse panustada.

Töö tulemused on sarnased varasemalt avaldatud uurimuste tulemustele ning need toetavad vajadust koordineerida küberturbet tarneahelas. Selline koostöö sisaldab lepingulisi kohustusi, minimaalsete investeeringute määra määramist ja info jagamist tarneahela ettevõtete vahel.

Töö tulemusi saab edaspidi kasutada uurimaks laiendatud mudelit, mis hõlmab rohkemat kui kahte ettevõtet, lisades võrgutopoloogia või küberkaitsekindlustuse. Ka otsustusprotsessi uurimine käitumusteaduslikust aspektist võib anda olulise panuse teemasse. Üheks olulisemaks tuleviku-uuringuks on mudelite empiiriline analüüs kasutamaks tegelike ettevõtete andmeid: nagu ka mitmed eelneva teoreetilised tööd, vajab selles magistritöös välja toodud mudel testimist tegelike andmete peal.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 55 leheküljel, 4 peatükki, 4 joonist, 1 tabelit.

Table of Contents

List of Figures

List of Tables

1. Introduction

Cybersecurity has become increasingly significant in firms' decision-making processes due to the rising number of cyber threats, which has sparked discussions on how to avoid disruptions in business operations. At the same time, real-world events – such as the COVID-19 pandemic, elections, the Olympic Games, and wars – have influenced the cyber landscape, as adversaries exploit such events to target vulnerable entities. This dynamic environment has prompted a substantial body of research focused on technical defences and solutions. However, the economic dimensions of cybersecurity remain underdeveloped. As noted by Kianpour *et al*. (2021), the economics of cybersecurity is still in its early stages, despite four decades of scholarly attention. They trace the origins of this field to 1982, when J. H. Courtney asserted that "security control should not be implemented if it costs more than tolerating the problem" ([19], p. 1).

According to Kianpour *et al.* (2021, p. 4), the most widely accepted definition of cybersecurity economics is "a field of study that is concerned with providing maximum protection of assets at the minimum cost." They further note that this discipline addresses decision-making within organizations – particularly concerning the valuation of assets and the allocation of scarce resources – under conditions of uncertainty. Economic theories are applied to cybersecurity issues, ranging from resource allocation and utility theory to strategic planning through game-theoretic models. In essence, cybersecurity economics seeks to explain and guide how organisations evaluate assets and allocate limited resources while adapting economic theories to uncertain, real-world environments [19].

Even though cybersecurity economics is a relatively nascent field, and while the body of literature applying economic models to cybersecurity problems remains limited, it is growing. The existing literature reflects diverse approaches. For instance, Huang *et al*. (2013) identify two main streams in the economics of information security investments. The first focuses on investment decisions using game theory, analysing how firms respond to and anticipate the actions of potential attackers aiming to access or damage information assets. The second stream is grounded in decision and expected utility theory, emphasising the risk and return analysis of cybersecurity investments.

However, as Moore (2010) observes, although cybersecurity often involves asymmetric information, this does not necessarily imply underinvestment in security. Instead, it may

indicate a misallocation of resources, where investments are not directed toward the most effective defences. Moreover, the increasing interconnectedness of service providers, individuals, and public sector organizations means that an attack on one entity can result in broader societal losses (*ibid*., p. 107). This interconnectedness can lead to a free-rider problem, in which firms underinvest in cybersecurity upon realizing others are also unlikely to invest, leaving the system collectively vulnerable [35]. In other words, if one firm in the shared IT system invests but others do not, the whole system is still vulnerable. Kianpour *et al*. (2021) similarly argue that when cybersecurity is treated as a public good, the classic "tragedy of the commons" problem emerges [19].

The main research question of this thesis is: What is the optimal level of cybersecurity investment for an interconnected, risk-neutral firm under uncertainty? To address this question, the thesis is structured as follows. Chapter 1 introduces the economic concepts underpinning cybersecurity economics, outlining the relevant theories used to model cybersecurity problems. It also reviews selected economic models concerning optimal cybersecurity investments.

In Chapter 2, the Gordon-Loeb model is extended by incorporating interconnectedness between firms. This model considers two firms that are interlinked and make decisions about their optimal cybersecurity investments. Initially, the model assumes perfect information – i.e., each firm knows the other's level of investment. Subsequently, imperfect information is introduced to better reflect real-world conditions, where firms typically do not know how much others are investing in cybersecurity. This leads to a framework similar to a Cournot oligopoly game, where firms make investment decisions simultaneously.

A response function is introduced to model this behaviour. Similar to a reaction function in a static model, this function assumes that firm i forms expectations about the investment level of firm j instead of knowing it precisely. The model is then extended to include dynamic elements, allowing for an analysis of the equilibrium outcome under uncertainty. To reflect real-world behaviour, a learning coefficient is incorporated into the function. This coefficient represents a firm's ability to learn and adapt over time, enabling the investment dynamics to evolve gradually. The key finding supports the free-riding problem discussed by Varian (2004): Firm 1 initially invests a small amount and gradually decreases its investment as it learns about Firm 2's investment levels.

Next the multiplicative interconnectedness is introduced where the economic meaning behind it is the means to enforce cybersecurity investments within supply chain. These can manifest in the form of legal contracts, regulatory instruments. Enforcing firms to invest into cybersecurity will benefit both of them – the substitution effect seen in previous model is eliminated and the level of cybersecurity is seen as join effort.

This thesis is written using available resources provided by University of Tartu and Tallinn Technical University. The text readability was improved by using Grammarly application.

1.1. Research questions

The primary objective of this thesis is to develop a model that describes the optimal level of cybersecurity investment for a risk-neutral, interconnected firm. This model serves as a tool to analyse the underlying mechanics of cybersecurity investment decisions and to explore how various external mechanisms – such as norms, regulations, or institutional settings—can enhance incentives for contributing to joint cybersecurity. To achieve this aim, we have posed the following research questions:

RQ1: What are the economic schools of thought that underpin theories related to cybersecurity?

This thesis addresses the intersection of cybersecurity and economics. The initial research question is designed to establish a foundational understanding by reviewing the literature on cybersecurity economics. The aim is to identify the most appropriate theoretical frameworks for analysing investment decisions in cybersecurity and to provide a comprehensive overview of existing studies that reflect diverse economic perspectives.

RQ2: What models have been developed to study optimal cybersecurity investment decisions?

The development of this thesis is based on prior research, providing a critical review of existing models. This inquiry identifies and synthesizes theoretical models that address optimal cybersecurity investment, establishing a foundation for further model development.

RQ3: Can existing models be adapted or extended to a setting involving two risk-neutral, interconnected firms?

Building on the literature review, this research question investigates whether and how existing models can be modified to accommodate a setting where two firms are both risk-neutral and interconnected. The thesis proposes extending the theoretical framework using a Cournot-type oligopoly game to capture the interdependent nature of cybersecurity investments in this context.

Answering those questions to reach the thesis's goal helps deepen the understanding of cybersecurity economics and provides insights into relevant policy measures or regulatory frameworks.

1.2. Scope and goal

In this thesis, we develop a theoretical model that captures the decision-making process behind optimal cybersecurity investments by risk-neutral firms operating in an interconnected environment. In today's digital economy, firms do not operate in isolation; their cybersecurity postures are interdependent due to shared infrastructures, supply chains, and data flows. Therefore, individual investment decisions may have externalities – positive or negative – on other firms. This thesis aims to model for such interdependencies to analyse dynamics behind investment decisions and provide insights to improve joint cybersecurity in supply chain.

The research focuses on the intersection of cybersecurity and economic theory, specifically utilizing concepts from cybersecurity economics and non-cooperative game theory. We employ a Cournot-type oligopoly framework to model the strategic interactions between two interconnected firms, which are assumed, in sake of simplicity, to be risk-neutral. Within this framework, the thesis explores how firms make cybersecurity investment decisions, considering that their actions influence and are influenced by the investment behaviours of the others.

The scope of the thesis includes a literature review of relevant economic theories related to cybersecurity, a survey of existing models that address optimal investment under risk neutrality, and the development of an extended model that incorporates interconnectedness. In this thesis, we do not seek or provide empirical validation but highlight the theoretical modelling and conceptual insights. Those can support future empirical studies and policy-making efforts aimed at enhancing collective cybersecurity outcomes.

1.3. Novelty

This thesis introduces a novel approach by extending the classical Gordon-Loeb model of optimal cybersecurity investment into a more realistic and strategically complex context involving two risk-neutral, interconnected firms. While the original Gordon-Loeb framework assumes a single, isolated decision-maker operating in a static risk environment, this thesis diverges from that model by explicitly incorporating inter-firm interconnectedness, which is increasingly relevant in today's digitally interdependent economies.

One of the contributions of this work is the introduction of strategic interactions among firms into the investment decision-making process. By framing the situation as a noncooperative game, the thesis foregrounds how the investment in one firm's cybersecurity impacts and is impacted by the other firm's investment decisions. This structure captures the externalities and interdependence in real-world cybersecurity environments, where one firm's weakness can propagate to another through connected systems or networks.

In addition, the thesis introduces yet another level of novelty by including incomplete information and learning mechanisms, we assume that firms do not have complete knowledge of their counterpart's behaviour or strategy and need to form and update beliefs over time. The dynamic component gives a more realistic representation of decision-making under uncertainty and allows the model to account for expectations formation and adaptive learning.

The findings of this thesis contribute to the theoretical development and may initiate changes in regulatory environments and increase incentives to promote collective cybersecurity resilience.

2. Literature review

In this chapter, we review a range of research papers that analyse economic models related to cybersecurity investment. The terms “cybersecurity economics,” “information security economics,” “economics of cybersecurity,” and “economics of information security” are often used interchangeably in the literature, despite subtle differences in meaning. To avoid missing relevant studies due to terminology, both “cybersecurity” and “information security” were used as search keywords. While these concepts are frequently combined, they are not identical. Cybersecurity has a broader scope, encompassing the protection of not just information assets but also human and cyber-physical systems [19]. According to ISO/IEC 27032:2012, cybersecurity includes information security, network security, internet security, and the protection of critical information infrastructure [16].

The articles included in the review were identified through a systematic search process using specific keywords. Terms such as “cybersecurity economics,” “economics of cybersecurity,” “economics of information security,” “information security economics,” and “cybernomics” were entered into the Google Scholar and ScienceDirect databases. This search produced a significant number of results. To reduce redundancy and enhance specificity, Boolean operators AND and OR were utilized. For instance, the search string “economics of cybersecurity” OR “economics of information security” generated approximately 151 results in Google Scholar and 180 papers in ScienceDirect.

To refine the search, the term “optimal investment” was added, which reduced the results to 147 in Google Scholar and 139 in ScienceDirect. Adding the term “literature review” further narrowed the results to 55 and 7 papers, respectively. These filtered papers formed the initial corpus for this literature review. Additionally, the snowball method – identifying further relevant studies from the references and citations of the initial articles – was employed to ensure comprehensive coverage of the field.

The remainder of this chapter is structured as follows. First, we examine how cybersecurity is conceptualised within various schools of economic thought. Then, we analyse selected economic models that determine optimal cybersecurity investment levels.

2.1. Economics of cybersecurity

One of the focus areas of cybersecurity economics is whether organisations are investing sufficiently in securing their assets and whether the resources allocated to cybersecurity are appropriately invested. When discussing cybersecurity investments, one should take into account the specific characteristics of these investments. For example, a typical investment into improving business processes may include building a new factory to increase revenues. However, cybersecurity investments are made to prevent or reduce possible losses caused by cybersecurity breaches. This feature complicates modelling the optimal investment figure as an organisation's resources are always scarce. The organisation should clearly understand the assets it wants to protect and the risks that may occur in a security breach. Kianpour *et al.* (2021) define cybersecurity economics as a study that claims to solve problems such as the following ([19], p 5):

1. What is the adequate level of cybersecurity, and how much should we spend on it?
2. How to provide cybersecurity? For whom?
3. Who needs to pay for interdependent risks?

However, the economic theory behind these questions includes assumptions about the environment where those questions are answered. Among others, there are assumptions about unlimited resources, complete information, rational choices, and operating in closed IT systems (not connected to others). However, these assumptions are frequently criticised for being unrealistic or overly simplistic. For example, unlimited resources are highly unrealistic - organisations face a scarcity of available funds, labour and time daily. This scarcity necessitates trade-offs: allocating resources to one objective may undermine the achievement of another. Consequently, limited resources emphasise the importance of making effective and strategically informed decisions.

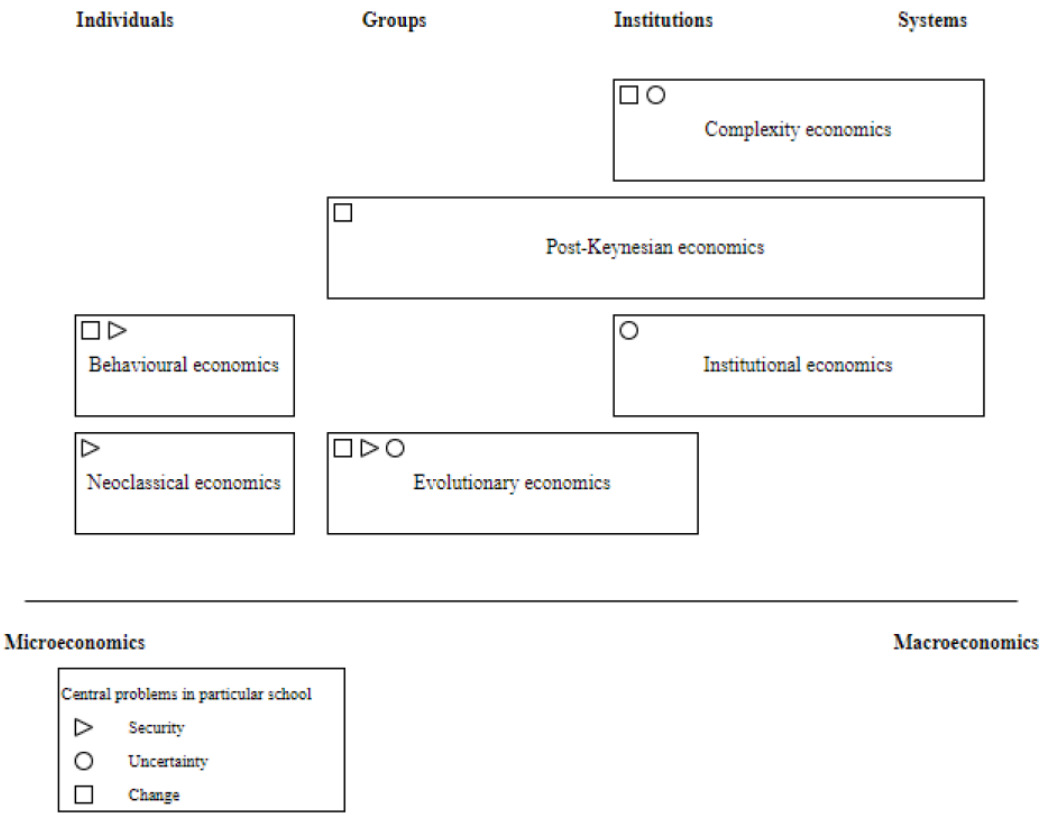

Figure 1. *Cybersecurity economics in economic schools (source: Kianpour et al. (2013))*

Figure 1 illustrates various schools of economic thought as they relate to cybersecurity. Neoclassical economic theory, one of the dominant paradigms in modern economics, focuses on allocating limited resources, efficiency, and maximising utility. Of particular relevance is the principle of achieving maximum utility from the use of scarce resources. Cybersecurity economics is a relatively new subfield that contributes to the broader economic discourse through both decision-theoretic and game-theoretic approaches. The former relies on traditional risk assessment models, while the latter conceptualises cybersecurity investment as a strategic interaction between attackers and defenders [19].

According to Huang *et al*. (2013), the game-theoretic approach is particularly well-suited for modelling the effectiveness of specific security technologies in finite action settings with a limited number of players – typically a defender (an organization) and an adversary. However, as Huang et al. (2013) note, this method foresees that one estimates the attacker's utility parameters, which may be complex and difficult task. Consequently, the game-theoretic approach has not been widely adopted for analysing cybersecurity investment decisions.

The decision-theoretic approach, by contrast, employs more conventional risk-return analysis and is better suited for determining the optimal level of cybersecurity investment across a range of security threats [15]. This branch's most widely cited model is the Gordon-Loeb model, which examines how an organization should determine its optimal cybersecurity investment level. This level is a function of the probability of a successful cyberattack without protective measures and the expected loss in the event of such an attack [19]. Subsequent chapters will discuss the model and its extensions in detail.

In both approaches, the main aim is to maximise utility. However, as Kayworth & Whitten (2012) argue, cybersecurity decision-making involves multiple objectives, including mitigating cyber risks, balancing business needs with security requirements, maintaining regulatory compliance, and ensuring alignment with organisational culture [18]. Moreover, the costs and benefits of cybersecurity investments are extremely difficult to quantify, as the benefits primarily stem from avoiding potential incidents and minimizing losses when breaches do occur [8].

While neoclassical economic theory provides a valuable foundation, it is not always well-suited to capture the complexity of cybersecurity investment decisions. Alternative schools of thought, such as behavioural economics, address some limitations by focusing on how decisions are made (see Figure 1). Behavioural economics integrates insights from economics, psychology, neuroscience, and cognitive science and demonstrates that individuals often deviate from the rational decision-making assumed in neoclassical models. Kianpour *et al*. (2021) identify three primary areas of deviation: (1) nonstandard preferences, including variations in time, risk, and social preferences; (2) nonstandard beliefs, like projection bias, overconfidence, and the law of small numbers; and (3) nonstandard decision-making behaviours, including framing effects, limited attention, menu costs, persuasion, social pressure, and emotional influences [19].

These behavioural factors can significantly affect cybersecurity investment decisions, given that individuals ultimately make such decisions. For example, Weishäupl *et al.* (2018) identified several external factors influencing information security decisions based on interviews with decision-makers in twelve organizations. These consist of national characteristics, laws, legal frameworks, and regulatory standards that impact organizations' motivation to invest in cybersecurity [36]. Similarly, industry practices and requirements by business partners also play a tremendous role. Their study also found that the majority of

organizations fail to accord adequate importance to information security, and they act only when forced by law. Notably, minimum levels of investment mandated by law are often unable to achieve the level of protection needed. [36]

In addition to behavioural economics, evolutionary economics offers an alternative to the neoclassical framework by addressing its key shortcomings. Evolutionary economics deals with complex systems, examining how and why economic structures change over time. It explicitly incorporates uncertainty and emphasizes the optimal use of scarce resources. In contrast to neoclassical theory – which often assumes systems gravitate toward equilibrium – evolutionary economics views systems as dynamic and path-dependent [31]. As Kianpour *et al.* (2021) point out, this perspective allows cybersecurity to be seen not merely as a constraint on change but as a potential enabler of business transformation.

Shiozawa *et al*. (2016) identify seven evolving, non-exclusive economic concepts central to this approach: economic behaviour, knowledge, organizations, commodities, systems, technology, and institutions. While individual behaviour may change through personal decision-making, institutional change generally requires broader societal consensus [31]. Shiozawa *et al*. (2016) illustrate this with the example of the Internet. Although it emerged as a new system, it quickly evolved in a decentralized manner, beyond the control of any single actor. Nonetheless, it remains a human-designed institution.

Beyond the aforementioned schools of thought, cybersecurity has also been examined through institutional economics, international economics, and international relations theory [19]. Kuerbis & Badiei (2017), for example, found that ex-post efforts such as botnet mitigation, route monitoring and other information-sharing initiatives can be effectively implemented under various combinations of governance structures [22]. Lindsay (2017) integrates international relations theory and institutional economics to conceptualize cyberspace as a global institution shaped by varying contractual frameworks in software and human behaviour. He argues that hackers often exploit vulnerabilities that stem from market failures, regulatory gaps, or incomplete contracts, thereby increasing the likelihood and severity of cyberattacks. According to Lindsay (2017), cyber conflict is less a chaotic struggle and more a form of strategic exploitation within a loosely regulated environment [26].

2.2. Economic models describing optimal cybersecurity investments

Cybersecurity investment decisions are made under significant uncertainty. As discussed in the previous subsection, various schools of economic thought have been employed to explain the complexities of cybersecurity-related decision-making. Numerous variables influence these decisions, and most researchers agree that they must be made in environments characterized by high uncertainty – where the nature, motivation, and timing of potential attacks are largely unknown.

In this subsection, we provide a more detailed examination of the models developed over the past two decades to address this issue. One useful categorization of existing models is proposed by Fedele & Roner (2022), who classify optimal cybersecurity investment frameworks into four main categories:

1. single-firm models,
2. multi-firm models, where firms do not compete in the product market but share a network,
3. multi-firm models, where firms are competitors but do not share a network,
4. multi-firm models, where competing firms operate within a shared network environment.

In this thesis, we look at single-firm models, multiple interconnected firms models, and models describing interconnected firms with asymmetric networks and the possibility of contagion. This division stems from the thesis goal of developing the optimal cybersecurity investment model for interconnected firms, and therefore, the Fedele & Roner (2022) proposed categories are used moderately.

2.2.1. Single firm, single period models

The Gordon-Loeb model (hereafter referred to as GL) is one of the most widely cited models in the study of optimal cybersecurity investment and falls under the first category in the classification proposed by Fedele & Roner (2022). The GL model provides a structured approach to managing risk by modelling reduced probability of a security breach as investment in cybersecurity increases. It employs an economic utility maximisation framework to analyse how firms allocate resources when facing two types of breach probability functions. The model is built on the assumption of scarce resources and assumes that the organization seeks to maximize economic benefit by allocating resources efficiently.

Gordon and Loeb (2002) incorporate game theory to examine interactions between attackers and defenders with limited resources. They ultimately estimate the optimal level of cybersecurity investment needed to minimise expected losses. A notable result of the model is that optimal cybersecurity investment does not exceed 36.8% of the expected loss. Additionally, they demonstrate that protecting moderately vulnerable information assets is the most efficient rather than the most or least vulnerable.

While the GL model is grounded in simplifying assumptions regarding attacker-defender behaviour and resource allocation, it remains a foundational framework for understanding trade-offs in cybersecurity investment and risk management. Over time, various scholars have extended the model to account for more realistic dynamics and scenarios.

For example, Hausken (2006) extends the GL model by introducing alternative breach probability functions characterized by diminishing returns. In his model, cybersecurity investment increases convexly with vulnerability until it reaches a threshold, after which the most vulnerable assets receive the greatest protection. Hausken (2007) demonstrates that for low-impact vulnerabilities, the optimal investment is zero; however, as vulnerabilities reach intermediate levels, investment increases, eventually growing concavely in absolute terms while decreasing convexly in terms of expected loss[1] [13]. This implies that, under specific breach scenarios, the optimal level of investment may exceed the 36.8% threshold proposed by the original GL model.

Huang *et al*. (2008) incorporate risk aversion into the GL model, distinguishing between two types of attacks: distributed (opportunistic) and targeted. Their model uses expected utility theory to assess investment decisions under varying risk preferences. They identify a minimum potential loss threshold, below which firms may not find it rational to invest in cybersecurity. Furthermore, Huang & Behara (2013) later show that increasing risk aversion among decision-makers does not necessarily lead to increased cybersecurity investment.

Willemson (2010) contributes by challenging the GL model's third assumption – that it is impossible to diminish the probability of a successful attack to zero, regardless of investment

[1] Here, the assumption of decreasing returns is set aside, and the assumption of logistically decreasing assumption for the security breach probability function is formed ($S(z, v)$ is logistically decreasing in z). The explanation is as follows: as investment increases from zero, the first impact is negligible. With increasing investment, the protection increases considerably. The impact eventually slows down as a firm has installed the best available system at some point.

level. Willemson (2010) argues that this assumption can be misleading, as some threats can indeed be eliminated through sufficient investment. He further contends that the 36.8% cap on optimal investment is not universally valid and may rise to 100% of the expected loss, depending on the vulnerability function selected [38].

In another extension, Huang & Behara (2013) incorporate budget constraints and network exposure into the GL framework. They find that network exposure significantly influences how firms allocate their cybersecurity budgets between mitigating targeted and opportunistic attacks. Under low exposure, it is more beneficial to focus on distributed threats, while high exposure environments warrant greater investment in protection against targeted attacks.

Krutilla *et al*. (2021) add a dynamics to the GL model by introducing both a capital discount and depreciation rates [20]. These parameters reflect the opportunity cost and lifespan of cybersecurity investments. They argue that the original GL model tends to underestimate optimal investment levels by assuming both rates are equal to one, thus inflating the user cost of cybersecurity assets. In their dynamic framework, where the rates are lower, user costs are reduced, making additional investment more economically viable and leading to higher optimal investment levels.

An emerging strand of literature also integrates cybersecurity insurance into the GL framework. Skeoch (2022) incorporates cyber insurance into the model to show how firms maximise utility under combined investment and insurance decisions. He shows that extending the GL model with cyber insurance can maximise expected utility, and insurance spending remains within the model's recommended threshold. According to this study, the balance between cybersecurity investments and cyber-insurance is shaped by several factors, including insurance premium rate, type of security breach function, firm's vulnerability level, and assumed utility function. In particular, lower premiums and higher risk aversion may lead to higher insurance coverage. At the same time, tighter cash constraints and more complex breach dynamics may lead the optimum toward direct investment. The study shows that full insurance coverage is optimal at reasonable premium rates and demonstrates that cyber insurance can complement traditional security investments cost-effectively [32].

Ebel & Mitra (2024) extend the GL model by introducing a two-sided Stackelberg game, in which the defender is modelled as the leader and the attacker as the follower [5]. Their results

show that the GL model underestimates optimal cybersecurity investment, particularly when the strategic behaviour of attackers is explicitly accounted for.

Table 1 below summarizes the key models of optimal cybersecurity investment developed by different authors. Most of these models build upon the foundational GL framework and contribute to the literature by relaxing assumptions, incorporating new variables, or adapting the model to dynamic or strategic settings. Nevertheless, as noted by several authors – including Skeoch (2022), Huang *et al*. (2013), and Hausken (2006) – the debate over the optimal level of cybersecurity investment is ongoing. Many existing models still overlook real-world complexities, such as supply chain interconnectedness and network topology, which are challenging to integrate into a single framework.

Table 1. *Models on optimal cybersecurity investments.*

Author(s)	**Base theory**	**Risk**	**Findings**
Gordon & Loeb (2002)	Economic benefit maximisation	Risk neutral	Propose that optimal cybersecurity investment should not exceed 36.8% of the expected loss without investment. Most efficient protection is allocated to moderately vulnerable assets.
Hausken (2006)	Economic benefit maximisation	Risk neutral	Extends GL model using alternative breach probability functions. Shows that with diminishing marginal returns, the optimal investment may exceed 36.8% for intermediate vulnerabilities; investment is zero for low vulnerabilities and constant for high vulnerabilities.
Willemson (2006)	Expected utility theory	Risk neutral	It uses linear probability functions to show that optimal investment may reach up to 100% of the expected loss, challenging the 36.8% upper bound.
Huang *et al.* (2008)	Expected utility theory	Risk averse	Extends GL model by incorporating risk aversion and attack types (targeted vs. distributed). Finds that optimal investment does not always increase with effectiveness or risk aversion. Identifying the primary threat is essential.[2]

[2] They distinguish two types of risks in decision-making: risk of loss from security breach and risk of over-investing, security risk and investment risk, respectively. From certain level of investments, the investment risk might eventually outweigh the security risk leading to a result that when the risk aversion coefficient α is very small or very high, the optimal investment into cybersecurity are small, i.e. the relationship between risk aversion and investments is concave. There exists a value for α at which the optimal investment is the highest.

Author(s)	Base theory	Risk	Findings
Willemson (2010)	Expected benefit maximisation	Risk neutral	It highlights inconsistencies in GL assumptions and proposes that the vulnerability function should be strictly increasing to reflect realistic investment behaviour.
Baryshnikov (2012)	Expected utility function	Risk neutral	Generalizes the GL model. Shows that for optimal investment, the probability function must be non-increasing and log-convex, confirming the 37% bound under specific conditions.
Huang & Behara (2013)	Expected utility theory	Risk averse	It considers budget constraints and network exposure. If resources are limited, it recommends allocating a budget to one attack type; in highly connected systems, greater investment should target the prevention of targeted attacks.
Gordon *et al.* (2014)	Economic benefit maximisation	Risk neutral	Extends GL model to account for security investment externalities (spillover effects) between interconnected firms.
Wu *et al.* (2015)	Economic benefit maximisation	Risk neutral	Develops a game-theoretic model, including attack types and network interdependence. Finds diminishing returns on investment and proposes incentive frameworks for inter-organisational settings.
Krutilla *et al.* (2021)	Economic benefit maximisation	Risk neutral	Adds a dynamic component to the GL model by including discount and depreciation rates. Finds that static GL underestimates optimal investment due to inflated user cost assumptions.
Skeoch (2022)	Economic benefit maximisation	Risk neutral	Integrates cyber insurance premiums into the GL model. Suggests that insurance can lead to underinvestment by altering perceived expected loss.
Ebel & Mitra (2024)	Max-min problem	Risk neutral	Introduces attacker side into GL model. The defender minimizes expected loss, and the attacker maximizes net gain. Finds that GL underestimates optimal investment in strategic settings.

The reviewed models on optimal cybersecurity investments build primarily on the GL model. Most studies assume risk-neutral firms and apply either economic benefit maximisation or expected utility theory. Gordon & Loeb (2002) originally proposed that optimal cybersecurity investments should not exceed 36.8% of expected loss without protection. Subsequent studies such as Hausken (2006) and Willemson (2006) challenged this bound by introducing alternative breach probability functions, showing that under certain conditions – like diminishing returns or linear vulnerabilities – optimal investment levels may be higher ([13], [37]). Other contributions incorporate risk aversion ([14], [15]), budget constraints, and network exposure, showing that optimal investment level does not necessarily increase with threat severity or risk preferences. Further extensions add externalities in interconnected firms [9], network interdependence and attack typologies [35], dynamic cost structures [20], and insurance premiums [32]. Ebel & Mitra (2024) introduce a strategic attacker into a two-sided game and show that the traditional model may underestimate the level of optimal cybersecurity investments [5]. In sum, these studies underscore the complexity of identifying the optimal level of cybersecurity investments in real-world environments where factors like spillovers, imperfect information, interdependence, and strategic interactions may cause substantial deviations from socially optimal levels of those investments.

2.2.2. Multiple interconnected firms models

The second category in Fedele & Roner (2022) introduces an additional layer to cybersecurity investment optimization models: interconnectedness and multiple firms. This category represents real-world conditions, as few firms operate in isolation. Fedele & Roner (2022) distinguish between various types of interconnectedness in their modelling framework: 1) firms that share a network but are not competitors, 2) firms that are competitors but do not share a network, and 3) firms that are both competitors and share the same network. In addition to modelling firm-level decision-making, they also explore welfare-oriented models that seek to identify socially optimal investment levels and compare them to privately optimal firm-level decisions. These themes align with Kunreuther & Heal (2003), who demonstrate that firms tend to underinvest in cybersecurity in interconnected IT systems due to positive externalities unless coordination mechanisms or policy interventions are introduced [23].

Roner (2022) focuses on a subcategory where firms share a computer network but are not product-market competitors. A real-world example of this type is illustrated by the 2014 Target data breach, which involved Target Corp., a major retail chain, and Fazio Mechanical Services

Inc., a heating, ventilation and air conditioning service provider. Though not competitors, the two companies were digitally interconnected – Fazio used Target's internal network for service provision. A spear-phishing attack on Fazio led to a system compromise, granting attackers access to Target's network and sensitive data [33].

Gordon *et al.* (2015) extend the original GL model by incorporating the external costs of cybersecurity breaches – namely, spillover effects on other firms. Their findings suggest that accounting for these externalities raises the optimal level of cybersecurity investment. This highlights a critical limitation of firm-level models that ignore interconnectedness: they may significantly underestimate the true social cost of cyberattacks.

Similarly, Wu *et al*. (2015) developed a game-theoretic model to analyse cybersecurity investments in interconnected firms, considering targeted and opportunistic/distributed attacks. They show that joint decision-making can reduce total expected losses in the case of distributed attacks, internalise network vulnerability externalities, and enhance overall security. For targeted attacks, firms should increase investment proportionally to intrinsic vulnerability and reconfigure their information systems if the vulnerability is moderate.

The foundational literature on technical spillovers in cybersecurity investment began with Kunreuther & Heal (2003), who proposed a game-theoretic model. They found that the incentive to invest in cybersecurity diminishes as the number of interconnected firms increases. In the limit, as the number of firms (N) approaches infinity, the incentive to invest tends toward zero. This effect, often called the free-rider problem, emerges because each firm relies on others to invest in protection, reducing their incentive to do so.

By contrast, economic studies on R&D investment in supply chains show that spillovers can have a positive effect. For instance, research by Li & Bosworth (2020) and Parast (2020) finds that a firm's R&D investment positively affects the productivity and innovation potential of other firms in the supply chain. These studies treat R&D as a value creation and capability development tool, especially in dynamic or uncertain environments. While cybersecurity investments differ in that they aim to prevent losses rather than create value, they, too, can generate positive spillover effects by enhancing network security for all members – reducing the probability of contagion.

As Fedele & Roner (2022) note, there is a growing body of literature building upon Kunreuther & Heal's (2003) foundational work. For example, Böhme (2012) models interconnected firms

exposed to both direct (own breach) and indirect (contagion) risks [3]. He demonstrates that the Nash equilibrium leads to underinvestment. Varian (2004) also discusses free-riding behaviour under three security scenarios: total effort, weakest link, and best shot[3]. In the total effort and best shot settings, a single agent with the best cost-benefit ratio provides most or all investment, while others free-ride [35]. However, these models often assume perfect information about other agents' behaviour – an assumption that may not hold in reality. Under imperfect information, free-riding may decrease, and leadership becomes more important in coordinating security decisions.

Grossklags & Christin (2008) expand this line of inquiry by distinguishing between self-insurance (e.g., data backups) and self-protection (e.g., firewalls) [12]. Their model assumes simultaneous decisions made by a single agent per firm. They find that self-insurance investments are always made at the socially efficient level, while self-protection investments may be suboptimal from a welfare perspective. This is because only self-protection measures produce positive externalities (technical spillovers), whereas self-insurance measures benefit only the individual firm.

In summary, applying cybersecurity investment models to account for inter-firm inter-connectedness reveals critical dynamics absent in single-firm analyses. Spillover effects, free-riding behaviour, and strategic interdependence are key in shaping investment incentives, particularly when firms are connected through networks or face common threats. While some investments generate positive externalities that enhance network security, others remain privately optimal but socially suboptimal.

These insights are the foundation in analysing the more advanced systems – specifically, asymmetric networks and contagion processes – in which firms differ in size, exposure, and connectivity and where the impact of one firm's failure can spread randomly throughout the system.

2.2.3. Asymmetric networks and contagion

Thus far, most studies discussed have assumed symmetric networks, where all agents interact with one another and occupy equivalent positions within the network. However, as Acemoglu

[3] In the weakest link scenario, the system reliability stems from the firm with the lowest benefit-cost ratio. Best-shot describes the scenario where the firm with the highest benefit-cost ratio contributes all the effort. Moreover, the total effort of the system reliability is determined by the firm with the highest benefit-cost ratio. [35]

et al. (2016) argue, this assumption is highly unrealistic. Their research emphasizes the importance of network structure in shaping cybersecurity investment decisions and introduces models based on asymmetric networks. They demonstrate that in such networks (e.g., star or hub topologies), strategic attackers may redirect their focus in response to overinvestment by specific nodes. When one agent increases its cybersecurity investment, it may inadvertently shift the attacker's attention to less-protected nodes. As a result, equilibrium investment levels may exceed the socially optimal level [1].

A related study by Dziubinski & Goyal (2017), building on a similar framework, shows that firms may be incentivized to invest in cybersecurity only when others do the same. This interdependence can result in coordination failure: although the socially efficient outcome would involve complete protection of the network, an equilibrium exists in which firms collectively underinvest [30].

Most of the literature thus converges on two core findings: first, in equilibrium, firms tend to underinvest in cybersecurity due to positive externalities and coordination failures; second, network structure plays a significant role, though it is often assumed to be exogenously given. However, in Dziubinski & Goyal (2013), network topology becomes a decision variable (as sited in [11]). Their model features a two-stage game in which the defender selects the network structure to maximize the total payoff across all firms, followed by a strategic interaction with the attacker. In this model, contagion between nodes is not permitted.

By contrast, contagion is explicitly modelled in the work of Goyal & Vigier (2014), who analyse a sequential game between a network designer and an adversary. They find that, in equilibrium, the network topology tends to converge to a star network or a multi-hub configuration, depending on the network value function, the technology of conflict, and the relative allocation of attack and defence resources. Their result shows that star networks, where all the defence resources are concentrated at the hub, can maximise expected value under high contagion risk and convex network value functions. In addition, they found that under alternative conditions like low conflict intensity or a flatter network value function, multi-hub configuration may be optimal. The work highlights the critical role of contagion dynamics and resource asymmetries that are important in shaping network architecture and cybersecurity investment strategies (see [11]).

The remaining two categories of models identified by Fedele & Roner (2022) fall outside the scope of this thesis and will not be discussed in detail. The third category addresses multi-firm models in which firms are competitors in the product market but do not share network infrastructure. This stream originates with Garcia & Horowitz (2002) (as cited in [30]). A relevant example is the e-commerce sector, where firms like Amazon and eBay compete but operate independent IT systems. The fourth category comprises firms that share network infrastructure and compete in the same market. Roner (2022) suggests that the banking sector is an example of this category, where institutions such as banks are in direct competition yet remain closely interconnected (e.g., via the Society for Worldwide Interbank Financial Telecommunication, SWIFT, network).

In terms of supply chain cybersecurity models, the literature remains relatively limited. While many studies have examined strategic interactions between attackers and defenders, few have explored game-theoretic dynamics between firms within supply chains. One notable exception is Nagurney *et al*. (2016), who developed a game-theoretic model in which firms – specifically retailers – compete noncooperatively to maximize profit, subject to nonlinear budget constraints that include cybersecurity investment. In their model, the probability of a successful cyber breach depends on the individual firm's cybersecurity level and the collective cybersecurity posture of the supply chain. One might suggest that the level of cybersecurity in the supply chain might be the case of coordination: coordination in supply chain cybersecurity can benefit from insights drawn from supply chain coordination, particularly in the context of foreign direct investment. Supply chain coordination mechanisms – contracts, information sharing, and joint investment – enhance firm resilience and performance [4]. When foreign firms invest in host countries, their security postures affect and are affected by local partners, making coordinated cybersecurity critical. Analogous to the bullwhip effect[4] in supply chains, a lack of coordination in cybersecurity may amplify risks across interconnected firms [24]. Thus, collective cyber resilience could benefit from fostering joint standards, shared threat intelligence, and investment incentives among firms.

Whereas the models described above give helpful insights into suitable levels of cybersecurity expenditure, they are limited in terms of empirical testing. Although the general opinion is that

[4] The bullwhip effect describes the phenomenon in supply chains where small fluctuations in consumer demand at the retail level lead to larger variations in orders and inventory levels. The effect is primarily driven by delays in information sharing, demand forecasting errors, order patching, and lack of coordination among supply chain partners [24]

firms do underinvest, these models cannot always give precise, individual firm-specific levels of expenditure. To address this gap, Brho et al. (2025) propose the Alpha Model, which estimates an upper bound for private-sector cybersecurity investments that reverses the optimal financing structure [2]. Their framework distinguishes investment and operational spending and links cost-benefit analysis with expected market value loss in a cyber breach. Although their primary focus is on large firms (e.g., Amazon, Walmart), the model's integration of financial metrics into cybersecurity investment decisions is a valuable contribution.

Moreover, they find that direct losses from cyberattacks represent only a tiny fraction of total loss – approximately 4% – with indirect losses, such as market valuation loss, constituting the remainder. This result is consistent with Kamiya et al. (2017), who estimate that for every dollar in direct losses, firms experience, on average, a market value loss is approximately 115 dollars. Based on a dataset of 307 cyberattacks between 2005 and 2017, their research emphasizes the severe economic effects beyond direct operational costs [17]. Similarly, in a systemic literature review reviewing the impact of cyberattacks on stock prices, Spanos & Angelis (2016) recorded that nearly ¾ of the studies reviewed identify a significant negative impact on firm value [34]. So, most cybersecurity investment models may underestimate the expected loss by focusing solely on direct costs. Gordon et al. (2016) further stress that measuring the economic impact of cybersecurity breaches requires considering both tangible and intangible costs. The latter consists of, for instance, reputational damage, legal liabilities, and the broader financial consequences reflected in market behaviour. These findings show that several existing cybersecurity investment models may underestimate expected losses by focusing narrowly on direct costs while ignoring the indirect consequences of cyber incidents.

This chapter considers the evolution of investment models describing cybersecurity investments, starting from the single-firm models like the GL model to the richer environments with interdependent and networked firms. Whereas earlier models had symmetric interaction and risk neutrality, recent studies focus on network structure, externalities, and strategic interdependence. Asymmetric networks, coordination failures and contagion risks create suboptimal investment levels, pointing out the shortcomings of noncoordinated decision-making. Theoretical advances aside, empirical testing of these models remains problematic, particularly for interdependent systems such as supply chains. This leads us to the next chapter, which focuses on the investment behaviour in a supply chain.

3. Optimal cybersecurity investments model

3.1. The Gordon-Loeb model

As previously mentioned, Gordon and Loeb introduced the first formal model addressing cybersecurity investment decisions in 2002. The model presented in this thesis builds upon and extends the original GL framework. Specifically, it introduces additional elements to reflect real-world complexity better.

The original GL model considers a single, risk-neutral firm evaluating whether to increase its cybersecurity investment over a single period. The firm holds one information set requiring protection – this could represent a customer database, an accounts payable ledger, intellectual property, or similar sensitive data. For the sake of simplicity, the model assumes only one type of threat to this information set. The key parameters characterizing the information set and the decision environment are outlined in the table below.

Table 2. *GL model parameters (Gordon & Loeb, 2002)*

Parameter	**Description**
λ	Loss in case of the breach in monetary terms. λ is assumed to be fixed and smaller than any large number M.[5]
$t \in [0,1]$	Probability of a cyberattack
$v \in [0,1]$	Vulnerability of the information set, i.e. probability of the breach on the information set if there is no additional security introduced. *v=0* when information set is completely secure and *v=1* when information set is publicly available.
$\lambda \cdot t \cdot v$	Expected loss of a breach on the information set in case of no additional investments to information security.
$L = t \cdot \lambda$	Expected loss in case of a breach of an information set.
$z > 0$	Monetary investment in information security (for given information set). Measured in same units as L.

[5] This model is not suitable evaluating protection of national assets or assets that when breached have catastrophic aftermath.

Parameter	Description
$S(z,v)$	Security breach probability function. Denotes the probability of a breach of an information set with vulnerability *v* and conditioned with the firm's investments to protect this information set *z*.
$EBIS(z) = [v - S(z,v)]L$	Expected benefits of investments in information security.
$ENBIS(z) = [v - S(z,v)]L - z$	Expected net benefit from investment in information security (EBIS less the cost of investment).

Every economic model requires a set of assumptions that, while abstracting from reality, help ensure the model's mathematical tractability and consistency. The Gordon & Loeb (2002) model is no exception. It includes several assumptions regarding the breach probability function *S(z,v)*, which describes the probability of a security breach as a function of the investment level *z* and the inherent vulnerability of the information set *v*. These assumptions are as follows:

A1. *S(z,0) = 0* for all *z*. This implies that if the information set is completely invulnerable (i.e., has no inherent risk), it will remain secure regardless of the level of investment.

A2. For all *v*, *S(0,v) = v*. This means that if no resources are invested in security, the probability of a breach equals the inherent vulnerability of the information set.

A3. For all $v \in (0,1)$ and all $z, S_z(z,v) < 0$ and $S_{zz}(z,v) > 0$, where $S_z$is a partial derivative with respect to z and S_{zz} is the second-order partial derivative. This assumption implies that increasing investment reduces the breach probability, but at a decreasing marginal rate.

Additionally, it is assumed that for all *v*, $\lim_{z\to\infty} S(z,v) = 0$, which indicates that the probability of a successful breach can be made arbitrarily small with sufficiently large investment.

Gordon & Loeb (2002) propose two functional forms for the breach probability function *S(z,v)*, both of which satisfy the above assumptions:

$$S^I(z,v) = \frac{v}{(\alpha z+1)^\beta} \quad , (\alpha > 0, \beta \in \mathbb{R}) \tag{1}$$

$$S^{II}(z,v) = v^{\alpha z+1} \quad , (\alpha > 0) \tag{2}$$

These functions are selected to reflect decreasing breach probability with increasing investment while ensuring that the functional properties (monotonicity, convexity, and limiting behaviour) align with theoretical expectations.

These breach probability functions are then used to determine the optimal level of cybersecurity investment, denoted as $z^*(v)$ by applying the first-order condition to the firm's expected net benefit from information security (ENBIS). This optimization identifies the investment level that maximizes the net gain from reducing breach probability, given the vulnerability *v* of the information set. That means the first-order condition is set as follows:

$$\frac{\partial ENBIS}{\partial z} = \frac{\partial[(v - S(z,v))L - z]}{\partial z} = 0 \qquad (3)$$

Assumption A3 implies that *S(z,v)* is strictly convex in *z* and therefore ENBIS is strictly concave in *z*. Rearranging (3) for optimal investments, *z**, we get:

$$-\frac{\partial S(z^*,v)L}{\partial z} = 1 \qquad (4)$$

Here, the left-hand side describes the marginal benefits of cybersecurity investments, and the right-hand side shows the marginal cost of those investments. This implies that one should invest in cybersecurity only up to the point where marginal cost equals marginal benefit (for a more detailed explanation, see [8]).

Using the first order condition (4), optimal cybersecurity investments *z*(v)* can be calculated for both of the security breach functions, equations (1) and (2). As shown in Gordon & Loeb (2002), for all the functions that satisfy the conditions A1 to A3, the optimal investment satisfies the inequality $z^* < vL$, where L represents the potential loss in the event of a successful breach. More specifically, they show that:

$$z^{I*}(v) < \frac{1}{e}vL \text{ and } z^{II*}(v) < \frac{1}{e}vL,$$

where *e* is the base of the natural logarithm, implying that optimal investment should not exceed approximately 36.8% of the expected loss without security measures[6].

[6] For Type I of breach probability functions we have optimal cybersecurity investments according to equation (4) as follows: $\frac{z^{I*}}{vL} = \frac{(\beta\alpha vL)^{1/(\beta+1)} - 1}{\alpha vL}$. Letting $x = \alpha vL$ the optimal cybersecurity investments can be rearranged thus: $\frac{z^{I*}}{vL} = \frac{(\beta x)^{1/(\beta+1)} - 1}{x}$. The maximum of this equation is reached when $x = (\beta + 1)^{\beta+1}\beta^{-2-\beta}$ and substituting this into optimal cybersecurity equation we get $\frac{z^*}{vL} = (\frac{\beta}{\beta+1})^{\beta+1}$. The right hand side of this equation is increasing in β

It is important to note a critical assumption underlying this result: the firm is assumed to possess a basic level of information security infrastructure. This may include access controls, security protocols, or personnel – such as an IT officer – dedicating part of their time to security-related tasks. This assumption is operationalized through the absence of fixed costs associated with initiating entirely new security investments [8].

3.2. Extending GL model with interconnectedness

As discussed earlier, the original GL model is a single-firm, single-period framework. This thesis extends the model to incorporate interconnectedness between two firms. There are some models using interconnectedness in extending GL model ([28], [39], [23], [3]), but their contribution is a bit different from the logic used here. For instance, Wu *et al.* (2015) and Kunreuther & Heal (2003) use probabilities in the breach probability function to add the network vulnerability into the model. Nagurney *et al.* (2016) include the average cybersecurity level across the supply chain to the breach probability function and Böhme (2012) uses the interdependent risk to analyse the optimal cybersecurity investments. Here we use a different approach by adding the partner's investments into the breach probability function together with interconnectedness parameter. Specifically, we consider two interconnected risk-neutral firms, each choosing how much to invest in cybersecurity, denoted by z_1 and z_2, respectively.

The investment decisions are made simultaneously, forming a noncooperative game between the two firms. These firms are not competitors in the product market; rather, the interdependence arises from a service relationship in which one firm provides services to the other. Initially, we assume that firms make decisions independently, with no cooperation or regulatory requirements imposed by one firm on the other regarding cybersecurity standards.

Similar to the original GL model, the probability of a security breach for each firm depends on its investment level. However, due to interdependence, this probability now also depends on the other firm's investment level. The modified breach probability function for firm i is given by:

---

and applying L'Hôspital's rule we get $\lim_{\beta\to\infty}\left(\frac{\beta}{\beta+1}\right)^{\beta+1} = \frac{1}{e}$. And since right hand side of equation $\frac{z^*}{vL} = (\frac{\beta}{\beta+1})^{\beta+1}$ is smaller than *1/e* and $z^* < (1/e)vL$. The value of e is approximately 2.71828 and the value of *1/e* is therefore approximately 0.36788 indicating that the optimal cybersecurity investments should be less than 36.8% of expected loss without any security measures. For detailed discussion see [8].

$$S_i(z_i, z_j, v_i) = v_i \cdot H(z_i + \gamma z_j), \quad (5)$$

where $z_i \neq z_j$, $H(z_i, z_j)$ is some function such that $S_i(z_i, z_j, v_i)$ satisfies the conditions A1 to A3[7] and $\gamma \in [0,1]$ denotes the degree of interdependence. A higher γ implies a greater positive externality from the other firm's investment. That is, when firm *j* increases its cybersecurity investment, it reduces the breach probability for firm i due to lower contagion risk.

Each firm seeks to maximize its expected net benefit from information security (ENBIS), which now incorporates this interdependence:

$$ENBIS_i(z_i, z_j) = [v_i - S(z_i, z_j, v_i)]L_i - z_i = [v_i - v_i \cdot H(z_i + \gamma z_j)]\, L_i - z_i =$$

$$[1 - H(z_i + \gamma z_j)]v_i L_i - z_i \quad (6)$$

where L_i is the potential loss for firm i in case of a successful breach. Each firm maximises its expected net benefit, ENBIS. Each firm $i \in \{1,2\}$ solves the following maximisation problem:

$$\max_{z_i \geq 0} ENBIS_i(z_i, z_j) = [1 - H(z_i + \gamma z_j)]v_i L_i - z_i \quad (7)$$

Assuming the function $H(z_i, z_j)$ takes the same form as the Type I breach probability function in Gordon & Loeb (2002), we write:

$$H(z_i, z_j) = \frac{1}{(\alpha(z_i + \gamma z_j) + 1)^{\beta}} \quad (8)$$

Substituting equation (8) into equation (6), the ENBIS function becomes:

$$ENBIS(z_i, z_j) = [1 - \frac{1}{(\alpha(z_i + \gamma z_j) + 1)^{\beta}}]v_i L_i - z_i \quad (9)$$

Equation (9) indicates that the expected net benefit from information security now depend also on the investments of the other firm. To find the optimal amount of cybersecurity investments of firm *i* we take the first-order condition with respect to z_i and we obtain:

$$\frac{\partial ENBIS(z_i, z_j)}{\partial z_i} = \beta \cdot v_i \cdot L_i \cdot (\alpha(z_i + \gamma z_j) + 1)^{-\beta - 1} - 1 = 0 \Rightarrow$$

[7] Even though Willemson (2006, 2010) and Hausken (2006) show that different security breach functions will not limit optimal cybersecurity investments at the same level as shown in Gordon & Loeb (2002), the functions are chosen to be the same as in Gordon & Loeb (2002) for the simplicity of the model presented in this thesis.

$$\left(\alpha(z_i + \gamma z_j) + 1\right)^{-\beta-1} = \frac{1}{\alpha \cdot \beta \cdot v_i \cdot L_i} \quad \Rightarrow \frac{1}{\left(\alpha(z_i+\gamma z_j)+1\right)^{\beta+1}} = \frac{1}{\alpha \cdot \beta \cdot v_i \cdot L_i}$$

$$\left(\alpha(z_i + \gamma z_j) + 1\right)^{\beta+1} = \alpha \cdot \beta \cdot v_i \cdot L_i \Rightarrow$$

$$\alpha(z_i + \gamma z_j) + 1 = (\alpha \cdot \beta \cdot v_i \cdot L_i)^{\frac{1}{\beta+1}}$$

Solving for z_i^*, the optimal investment for firm *i*:

$$z_i^* = \frac{(\alpha \cdot \beta \cdot v_i \cdot L_i)^{\frac{1}{\beta+1}} - 1}{\alpha} - \gamma z_j \qquad (10)$$

Equation (10) illustrates that firm i's optimal cybersecurity investment is influenced not only by its vulnerability and potential loss but by the investment level of firm j, moderated by the interdependence factor γ. As the degree of interconnectedness increases, firm i can reduce its investment in anticipation of firm j investing more – reflecting a strategic substitution effect and giving rise to a potential free-riding problem. This outcome is consistent with the findings of earlier studies on interdependent security (see Chapter 2.2.2). The model applies especially when companies do not have formal coordination instruments such as contractual agreements or regulatory mandates in place. Under a decentralised environment, companies operate autonomously, primarily focusing on their cost-benefit analysis and seeking to minimise security spending while still using the benefits of others' security investments.

This relationship can be visualized through graphs showing how changes in γ affect optimal investment levels. We set vulnerability v_i to be 0.6, α is set to 0.0001, β to 1, and firm *i* expected loss in case of the breach L_i is 400 000. Next figure shows how the optimal investments change in case of different values of γ.

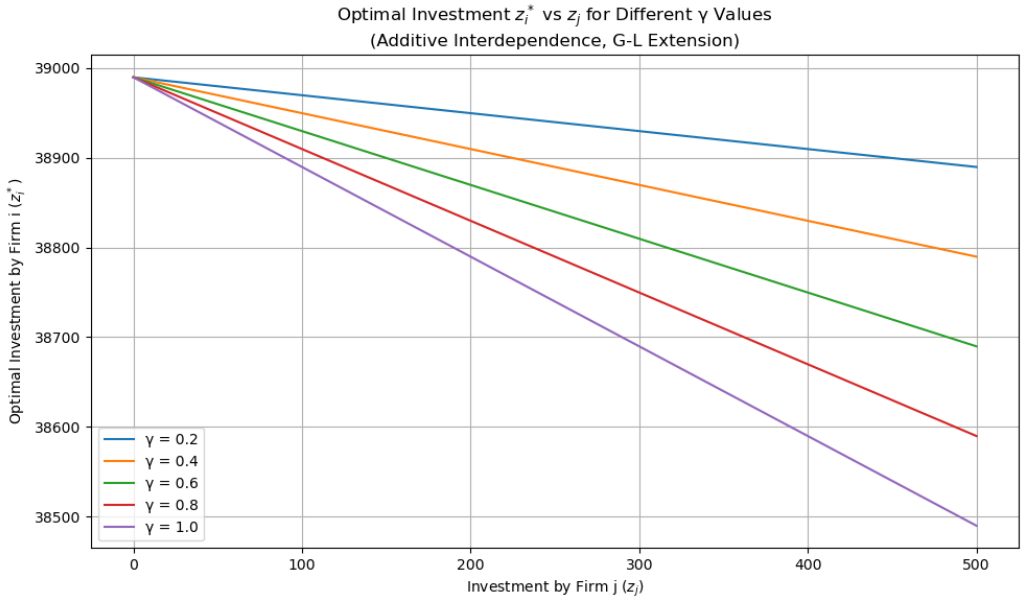

Figure 2. *Optimal cybersecurity investments of firm i and firm j in case of different interdependence.*

Figure 2 illustrates the problem of strategic substitution in cybersecurity investments. Given perfect information, firm *i* determines its optimal investment based on its vulnerability, expected loss, and model parameters – while observing the investment level of firm *j*. As shown, the more firm *j* invests in cybersecurity, the less firm *i* find it optimal to invest. This inverse relationship reflects a free-riding incentive typical in interdependent security settings. A more detailed analysis of this behaviour under the assumption of perfect information is provided in the Appendix.

The model presented in this subsection demonstrates that assuming additive interdependence in cybersecurity investments in the supply chain leads to a strategic substitution effect. However, the additive formulation might be the simplistic representation of real-world cybersecurity interdependence. In practice, if one interconnected firm fails to invest in cybersecurity, it can expose the entire supply chain to cyber risk, regardless of how much the other invests. Before extending the GL model to reflect the reality better, we take a closer look at the current framework by introducing the learning rate – which governs how a firm updates its expectations about the other firm's investment, given that these choices are not directly observable. The following chapter considers the current model in the context of a Cournot model with learning dynamics.

3.3. Imperfect information: A Cournot game with learning dynamics

In this chapter, we assume a setting of imperfect information, where firms do not observe each other's investment levels directly but instead make a guess about them. This transforms the model into a Cournot-style game in which each firm forms expectations about the other's investment. In addition, the model now has a dynamic element – changes take time.

Suppose firm i does not observe the firm j's investment directly but instead forms an expectation $\hat{z}_j$. The expectation $\hat{z}_j$ may be based on heuristics, past investment levels, or noisy observations. Then the response function becomes:

$$z_i^* = max\left(0, \frac{(\alpha \cdot \beta \cdot v_i \cdot L_i)^{\frac{1}{\beta+1}} - 1}{\alpha} - \gamma \hat{z}_j\right) \quad (11)$$

Equation (11) reflects real-world conditions in which cybersecurity investments are rarely public knowledge, and firms have to expect at least some amount of investments are made by another firm.[8]

Equation (11) gives the best response of firm i to the firm j´s investment expectations – it maximises its investments knowing its vulnerability, expected loss and expecting other firm to invest some amount. If a firm i assumes that other firm does not invest, it will choose its best response accordingly. Then, the result will be the same as that of the classical GL model without interconnectedness. However, suppose a firm believes the other firm will invest a considerable amount. In that case, it might decrease its willingness to invest, which means there is room for underinvestment due to the perception of other firm's actions.

If we add learning to the model, i.e. firms can observe other firm's actions and adjust their belief about other's investment accordingly, we need to introduce that into the model. Let $\eta \in (0,1]$ represent the learning rate of firm i in guessing the firm j investments, where a low η implies conservative adaptation (e.g., due to bureaucratic inertia or uncertainty), and a high η reflects rapid adjustment. This learning rate η captures the firm's ability to adapt the knowledge of other firm's investments and adjust its expectations accordingly. If a firm is uncertain about others´ behaviour, it might choose a smaller η to avoid overreacting (more conservative approach).

[8] Here, we still do not consider the possibility of contracts or legal requirements that might induce both firms to invest.

The dynamic learning-adjusted response function is[9]:

$$z_i^{t+1} = max\left((1-\eta)\cdot z_i^t + \eta \cdot max\left(0, \frac{(\alpha\cdot\beta\cdot v_i\cdot L_i)^{\frac{1}{\beta+1}}-1}{\alpha} - \gamma \hat{z}_j{}^t\right)\right) \quad (12)$$

This expression captures the bounded rationality of firms' actions – firms do not optimize immediately but approximate their behaviour over time. In other words, this expression captures how firm i gradually updates its investment decisions based on evolving beliefs about firm j's behaviour. It also introduces the possibility of persistent underinvestment or strategic free-riding, depending on initial beliefs and the value of η, echoing concerns raised by Varian (2004). However, adding learning dynamics to the model does not remove the substitution effect, and the result can approach Nash equilibrium as the adjustment happens (gradual convergence).

There are two distinct ways to visualize the strategic dynamics of cybersecurity investment: one assumes that the firms are identical – with symmetric values of the parameters like vulnerability and expected loss – while the other allows for asymmetry between these dimensions. The following figure illustrates the optimal cybersecurity investment levels for the symmetric case, where both firms in the supply chain share the same risk parameters. These investment levels are shown as a function of the degree of interconnectedness γ. The parameter *A*, which defines each firm's base incentive to invest, is calculated as follows:

$$A = \frac{(\alpha\beta vL)^{\beta+1}-1}{\alpha} \quad (13)$$

A is found similarly to perfect information case presented in Appendix 1. Here, the outcome for both firms is the same (as the parameters are identical). According to the model, the more interdependent the firms are, the less they tend to invest in cybersecurity. Following figure 3 shows the model without learning rate.

[9] Here, the maximisation is used to avoid the negative outcomes: inner max ensures that the best response function is nonnegative and outer max ensures that the learning update is also nonnegative.

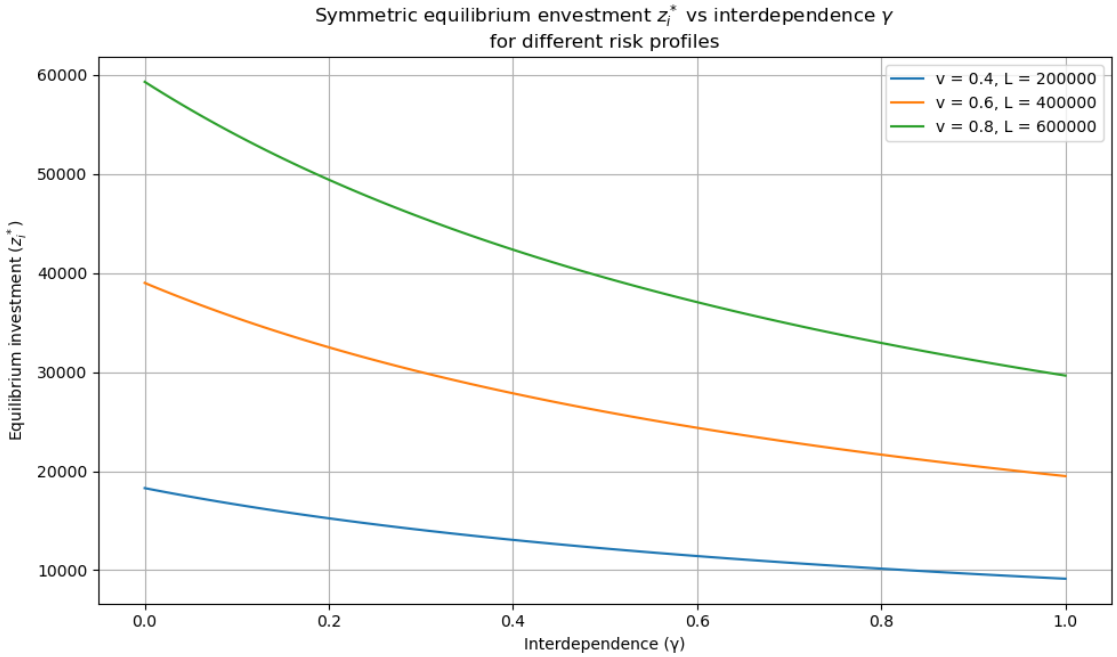

Figure 3. *Relationship between optimal cybersecurity investments and interdependence, the case of identical firms, different risk profiles.*

Adding learning rate ($\eta = 0.2$) to the model we get following results depicted in Figure 4. Here, the lines are reaching the equilibrium in time.

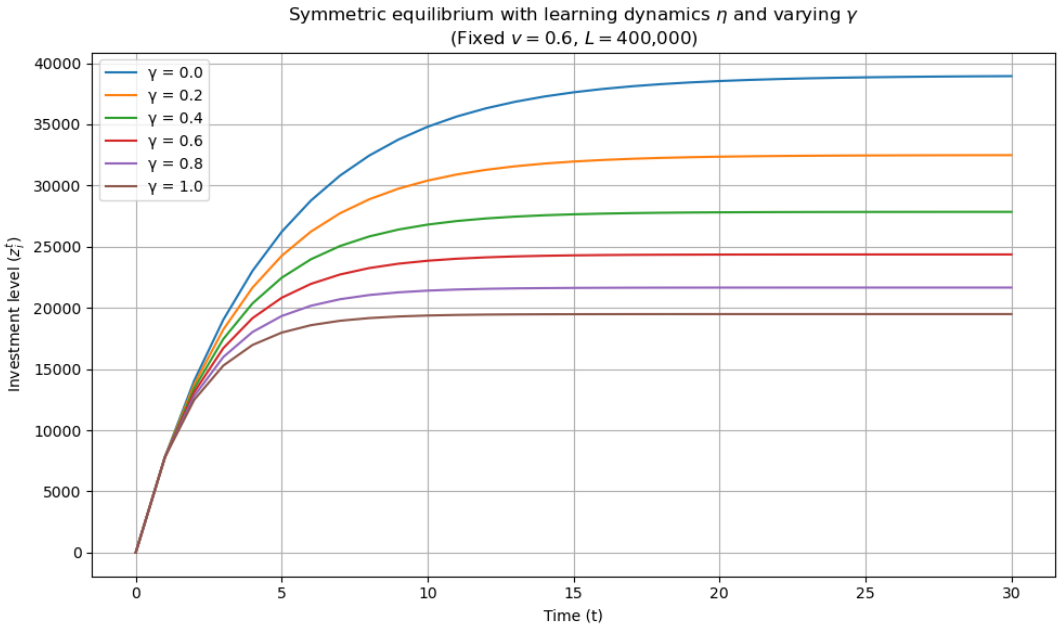

Figure 4. *Symmetric equilibrium with learning rate (identical firms)*

However, in practice, finding two identical firms within a supply chain is rare. Firms often differ in their vulnerability to cyber threats and the expected loss from the breach. To reflect this, we now turn to the asymmetric case for what we generate some numbers. Let vulnerability

for Firm 1 be 0.4, and that of Firm 2 be 0.7. Their respective expected losses are set to 300 000 and 500 000. Learning rate η is assumed to be 0.2, parameters $\alpha = 0.0001$ and $\beta = 1$. The degree of interconnectedness γ is set at 0.6. Figure 4 captures the investment dynamics under these conditions, using the additive interdependence model with learning.

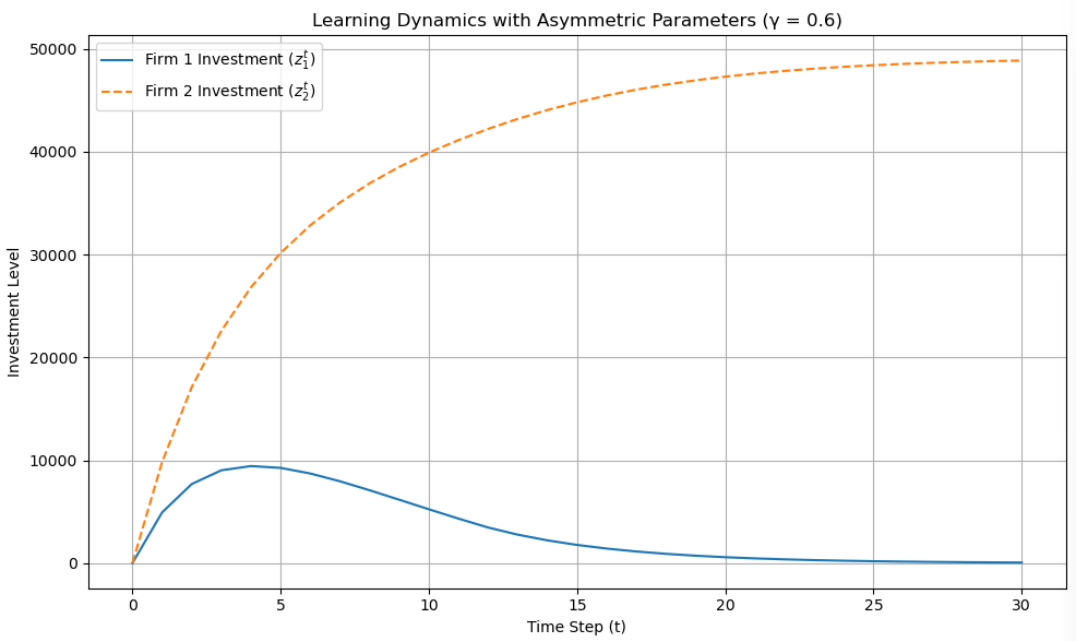

Figure 5. *Optimal cybersecurity investments in case of interconnected firms with learning rate.*

Figure 5 captures the strategic substitution effect in case of asymmetric parameters of the model – Firm 1, learning about Firm 2 investments, will gradually decrease its own. The lines presented on the Figure 5 differ due to the different parameters used – Firm 2 has higher vulnerability and expected loss and therefore invests more. However, Firm 1 gradually decreases its cybersecurity investments as its prediction of Firm 2's investment level improves over time and relies more and more on Firm 2' investments.

In sum, this additive model with learning illustrates how firms gradually adjust their cybersecurity investments based on expectations about their interconnected partners. While the model highlights the strategic substitution effect – where increased investment by one firm reduces the incentive for the other to invest – it also reveals how learning dynamics affect the convergence toward equilibrium. The simplicity of the additive framework provides a valuable benchmark to help see the decision-making process in the benefit maximisation framework. However, it may overlook key vulnerabilities in real-world interdependent systems, mainly when firms rely too heavily on their partners. In the next chapter, we explore a more realistic

formulation by introducing multiplicative interdependence, where joint investment is essential for adequate protection.

3.4. Cournot game in case of multiplicative interdependence

Up to this point, interdependence in cybersecurity investment has been modelled using an additive approach, where one firm's investment is directly added to the other, scaled by a parameter capturing the degree of interconnection. As the previous chapter shows, this additive structure often leads to a free-riding behaviour. When one firm knows its partner is investing in cybersecurity, it may be tempted to decrease or eliminate its efforts. This aligns with findings from earlier studies (see chapter 2.2.2). Therefore, we now adopt a different assumption: the two firms' investments are treated as complementary – the cybersecurity of the supply chain depends on the joint product of their efforts. This more realistic view echoes that coordinated protection can be enforced through contracts, legal obligations, or supply chain agreements in real life. Accordingly, we define the breach probability function for firm *i* as:

$$S_i(z_i, z_j, v_i) = v_i \cdot H(z_i \cdot \gamma z_j), \tag{14}$$

where $z_i \neq z_j$, $H(z_i, z_j)$ is a strictly decreasing breach probability function, defined such that the overall probability of a breach for firm *i*, $S_i(z_i, z_j, v_i)$, satisfies the assumptions of GL model A1 to A3 outlined in chapter 3.1. The parameter $\gamma \in [0,1]$, again, denotes the degree of interdependence – that is, how much the cybersecurity investment of firm *j* influences the security of firm *i*. High value of γ indicates that when the firm *j* increases its investment, it reduces the breach probability for firm *i*, due to lower contagion risks and therefore enhancing the overall security of the supply chain.

$H(z_i, z_j)$ is some function such that $S_i(z_i, z_j, v_i)$ satisfies the conditions A1 to A3 and $\gamma \in [0,1]$, again, denotes the degree of interdependence. $H(z_i, z_j)$ is strictly decreasing breach probability function. That is, if γ is high and when firm *j* increases its cybersecurity investment, it reduces the breach probability for firm i due to lower contagion risks. It increases the overall security of the supply chain.

As before, both firms aim to maximize its expected net benefit from information security (ENBIS). ENBIS now incorporates the multiplicative interdependence between the firms:

$$ENBIS_i(z_i, z_j) = [v_i - S(z_i, z_j, v_i)]L_i - z_i = [v_i - v_i \cdot H(z_i \cdot \gamma z_j)]\, L_i - z_i =$$

$$\left[1 - H\left(z_i \cdot \gamma z_j\right)\right] v_i L_i - z_i \quad (15)$$

Here, L_i is the potential monetary loss for firm i in the event of a successful breach. Each firm seeks to maximise its expected net benefit, ENBIS, taking into account the interdependence captured by the multiplicative breach probability function. Specifically, for each firm $i \in \{1,2\}$, the optimisation problem becomes:

$$\max_{z_i \geq 0} ENBIS_i\left(z_i, z_j\right) = \left[1 - H\left(z_i \cdot \gamma z_j\right)\right] v_i L_i - z_i \quad (16)$$

Assuming the function $H(z_i, z_j)$ follows the same structure as in the previous chapter's, we define it as:

$$H(z_i, z_j) = \frac{1}{(\alpha(z_i \cdot \gamma z_j)+1)^{\beta}} \quad (17)$$

Substituting equation (17) into the expected net benefit function (equation (15)), we obtain:

$$ENBIS\left(z_i, z_j\right) = [1 - \frac{1}{(\alpha(z_i \cdot \gamma z_j)+1)^{\beta}}] v_i L_i - z_i \quad (18)$$

Equation (18) highlights that firm *i*′s optimal investments depend directly on the firm *j*′s investment. This formulation reinforces that adequate security requires joint effort in an interconnected supply chain. If firm *i* invests, but firm *j* does not, the overall impact on cybersecurity is negligible. However, when both firms invest, the breach probability decreases significantly, creating mutually reinforcing incentives and eliminating the free-riding problem observed in the additive case.

Taking the first-order condition with respect to z_i, we obtain:

$$\frac{\partial ENBIS\left(z_i, z_j\right)}{\partial z_i} = \beta \cdot v_i \cdot L_i \cdot \left(\alpha(z_i \cdot \gamma z_j) + 1\right)^{-\beta-1} - 1 = 0 \Rightarrow$$

$$\left(\alpha(z_i \cdot \gamma z_j) + 1\right)^{-\beta-1} = \frac{1}{\alpha \cdot \beta \cdot \gamma \cdot z_j \cdot v_i \cdot L_i} \Rightarrow \frac{1}{\left(\alpha(z_i \cdot \gamma z_j)+1\right)^{\beta+1}} = \frac{1}{\alpha \cdot \beta \cdot \gamma \cdot z_j \cdot v_i \cdot L_i}$$

$$\left(\alpha(z_i \cdot \gamma z_j) + 1\right)^{\beta+1} = \alpha \cdot \beta \cdot \gamma \cdot z_j \cdot v_i \cdot L_i \Rightarrow$$

$$\alpha(z_i \cdot \gamma z_j) + 1 = (\alpha \cdot \beta \cdot \gamma \cdot z_j \cdot v_i \cdot L_i)^{\frac{1}{\beta+1}}$$

Solving for z_i^*, the optimal investment for firm *i* becomes:

$$z_i^* = \frac{(\alpha \cdot \beta \cdot \gamma \cdot z_j \cdot v_i \cdot L_i)^{\frac{1}{\beta+1}} - 1}{\alpha \cdot \gamma \cdot z_j} \quad (19)$$

Equation (18) shows that firm *i*′s investments depend directly on firm *j*′s investments: the value of firm *j*′s investment, z_j, appears in both the numerator and denominator of the expression, indicating that firm *j*′s investment increases firm *i*′s incentive to invest, but with diminishing returns. In contrast to the additive model discussed in the previous chapter – where investments function as strategic substitutes – the multiplicative structure here treats cybersecurity investments as strategic complements. If firm *j* does not invest, the firm *i*'s investment becomes meaningless, as overall breach probability remains high.

This complementarity eliminates the free-riding incentive observed in the additive case. Theoretically, cybersecurity in this framework can be viewed similarly to innovation investments: the more one firm in a supply chain contributes, the more others are encouraged to do the same (see [25], [29]). Furthermore, the interdependence parameter magnifies these incentives. The more interconnected the firms are, the more each firm's security depends on its partner's investment. In an interconnected environment, no single firm can invest heavily and remain secure in isolation – effective protection demands joint effort.

Compared to the additive model in the previous chapter, the firm *i*′s investments will turn meaningless if firm *j* is not investing. So, if in the previous additive model, investments can be viewed as substitutes, then in this model, those investments are complements, not allowing free-riding. This way, captured cybersecurity might be interpretable as innovation investments – the more one member of supply chain invests, the more it encourages others to invest. In addition, interdependence also appears in the equation, which magnifies the incentive: the more interconnected the firms are, the more the protection against cyber threats depends on other firm. In an interconnected world, one firm cannot invest heavily in cybersecurity and be protected and secure.

However, if both firms decide not to invest in cybersecurity, it might become another suboptimal solution – this model does not prevent this solution (similarly to Prisoners Dilemma).

Let us assume that we have two firms with different risk profiles. Firm 1 has a vulnerability set to 0.4; for Firm 2 it is set to 0.7. Expected losses for firms are 300 000 and 500 000,

respectively. We assume that firms are interdependent, and the value for γ is set to 0.6 and parameters $\alpha = 0.0001$ and $\beta = 1$. The best response functions for those firms are given by:

$$z_1^* = \frac{(\alpha \cdot \beta \cdot \gamma \cdot z_2^* \cdot v_1 \cdot L_1)^{\frac{1}{\beta+1}} - 1}{\alpha \cdot \gamma \cdot z_2^*} \tag{20}$$

$$z_2^* = \frac{(\alpha \cdot \beta \cdot \gamma \cdot z_1^* \cdot v_2 \cdot L_2)^{\frac{1}{\beta+1}} - 1}{\alpha \cdot \gamma \cdot z_1^*} \tag{21}$$

Nash equilibrium satisfies the system of those best response functions.

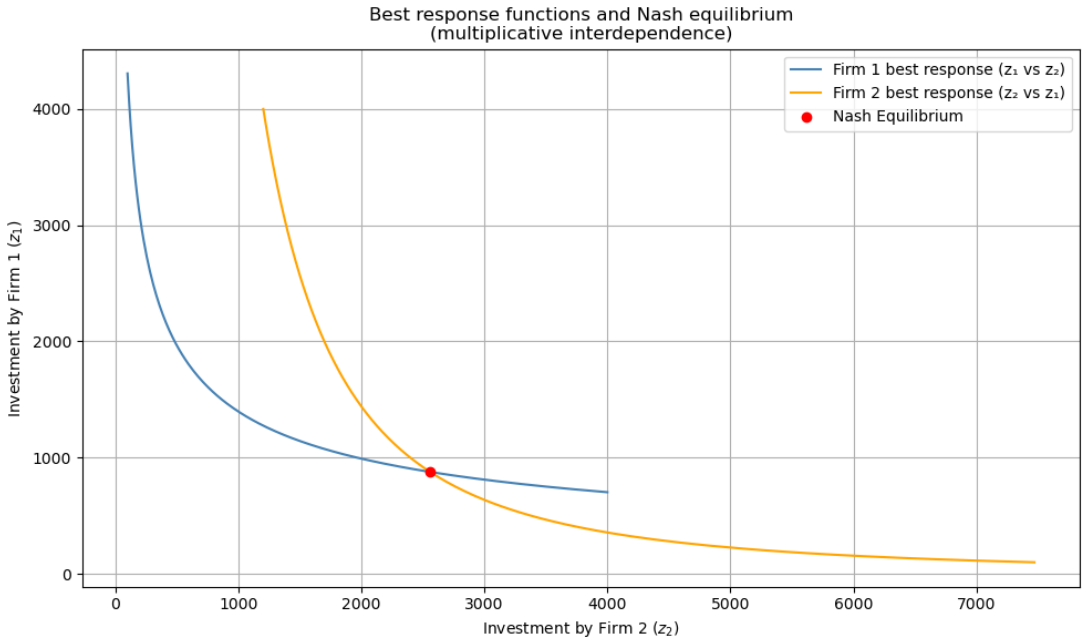

Figure 6. *Best response functions and Nash equilibrium.*

Figure 6 presents the best response functions for two asymmetric firms regarding multiplicative interdependence in cybersecurity investment. The blue curve represents the Firm 1's best response to Firm 2's investment z_2, while the orange curve captures the Firm 2's best response function to Firm 1's investment, z_1. The red dot marks the Nash equilibrium, where both firms simultaneously choose optimal investment levels given the other's decision.

The equilibrium point reflects that neither firm can achieve adequate cybersecurity protection unilaterally – the breach probability function is multiplicative. Therefore, each firm's investment is only effective when complemented by the other's efforts. As such, the equilibrium captures the mutual reinforcement of cybersecurity incentives in an interconnected world. Firm 2, which faces higher vulnerability and potential loss (v_2 = 0.7, L_2 = 500 000)

invests more than Firm 1, whose risk exposure is lower. Thus, this equilibrium reflects complementarity and heterogeneity in risk profiles.

This visual representation confirms the theoretical insight that cybersecurity investments are strategic complements under multiplicative interdependence, and optimal protection requires joint commitment across the supply chain. This aligns with the Weishäupl *et al.* (2018) survey, which found that the motivation for cybersecurity investments of interviewed decision-makers stems from laws, regulatory standards, and legal frameworks [36]. Our results with multiplicative interdependence as a contract between supply chain partners to increase joint cybersecurity, supporting this survey's result.

4. Conclusion

This thesis looks into how firms decide how much to invest in cybersecurity, especially when connected to other firms and operating under conditions of uncertainty and risk neutrality. The starting point for the analysis is the well-known Gordon-Loeb (GL) model, which serves as a baseline for understanding how a single firm should allocate resources to cybersecurity based on the potential losses and vulnerabilities of its information assets.

The GL model continues to give relevant insights into how firms see their appropriate level of cybersecurity investments and the best way to allocate those investments between different information sets. The most important variable in the model is the value of the information set, as it captures the potential loss in case of a cyber breach. As network segmentation to segment information sets is significant in cybersecurity, a firm will have more than one information set to protect. Another important variable in the model is the vulnerability of an information set, indicating that a firm needs to estimate the probability that this information set will be breached (for all information sets).

In this thesis, we extend the GL model in several critical directions to better reflect real-world interdependence, strategic behaviour, and imperfect information in cybersecurity. The first extension incorporates interconnectedness between two firms, modelling their investment decisions as a noncooperative game. Under perfect information, each firm optimally chooses its investment while knowing the other's choice. Results confirm a classic strategic substitution effect: the more one firm invests, the more reluctant the other is to do so. This introduces free-riding risk, particularly in the absence of coordination regulation.

To make the model more realistic, we introduced the concept of imperfect information and modelled the interaction as a Cournot game with learning dynamics. Here, firms form expectations about their partner's investment and adjust their behaviour iteratively using the learning coefficient (η). Simulation results indicate that the learning slows the adjustment toward equilibrium but does not eliminate the substitution effect. Over time, the learning process converges toward a stable outcome, but underinvestment remains a persistent risk, especially when initial beliefs or learning rates are misaligned.

Recognising that the additive interdependence may oversimplify the supply chains in real life, we introduced the final extension: a multiplicative interdependence model, where effective

cybersecurity depends on the joint effort of both firms. This setup changes the nature of the game: instead of strategic substitutes, investments in this setting are now strategic complements. In other words, one firm's investment increases the other's incentive to invest. Free-riding is no longer viable – if one firm fails to invest, the other's investment becomes negligible. The Nash equilibrium in this setting reflects both complementarity and heterogeneity in firm risk profiles, indicating that firms with higher risks optimally invest more.

The multiplicative interdependence model developed in this thesis offers a more realistic representation of the interdependencies commonly observed in supply chains, where firms are linked through contractual obligations, legal frameworks, and shared exposure to cyber risks. This approach also resonates with principles from innovation economics, where the investment of one actor can stimulate responsive action from others, leading to broader collective benefits. However, even this model assumes a relatively stable and known network topology that may not hold in volatile digital ecosystems.

Based on this thesis findings, it is evident that inter-firm interdependence in cybersecurity necessitates coordinated approaches to investment. The extended models demonstrate that firms are prone to free-riding under additive interdependence, especially in the absence of formal agreements or regulatory mandates. By contrast, the multiplicative interdependence model shows that joint investment mechanisms eliminate the free-riding problem and lead to more socially optimal outcomes, where one firm's investment strengthens the incentive for the other to invest.

To address the challenges described before, companies that share IT systems with partners should consider improving the baseline cybersecurity standards within the company and promoting contractual obligations within supply chains to enforce mutual investment. Tax incentives or subsidies could be useful to encourage firms, especially SMEs, to exceed the minimum investment threshold foreseen by law. In addition, a more coordinated approach to supply chain cybersecurity might increase the joint investment, as better coordination should be accompanied by improved information sharing and transparency. These measures help firms and supply chains move towards a strategic approach to mutual cyber resilience.

Even though this thesis enhances the existing framework of cybersecurity investments incorporating interdependence and learning, several possible future research topics remain. Extending the model by more than two firms and adding explicit network topology might shed

more light on contagion risks within a supply chain. Second, regulatory interventions, such as minimum investment requirements, liability rules or tax incentives, could add relevant insights to the model results regarding equilibrium outcomes and social welfare. Third, one could explore the landscape of cyber insurance and budget constraints within this model to add more comprehensive cost-benefit analyses to the model. Fourth, incorporating behavioural economics into the model, such as biases in decision-making, overconfidence, or limited attention, could help to understand different cybersecurity strategies. Last but not least, empirical calibration attempts to increase the practical relevance of the model - it could use the firm-level breach data, security investment levels or insurance claims to validate assumptions and condition policy recommendations.

References

1. Daron Acemoglu, Azarakhsh Malekian, Asu Ozdaglar. *Network security and contagion*. Journal of Economic Theory 166 (2016), pp 536-585, [accessed 23.01.2025], https://www.sciencedirect.com/science/article/abs/pii/S0022053116300837?via%3Dihub
2. Mazen Brho, Amer Jazairy, Aaron V. Glassburner, *The finance of cybersecurity: Quantitative modelling of investment decisions and net present value.* International Journal of Production Economics 279, 2025, 109448; [accessed 12.02.02.2025]; https://www.sciencedirect.com/science/article/abs/pii/S0925527324003050?fr=RR-2&ref=pdf_download&rr=9233a8c55d935433
3. Rainer Böhme. *Security Audits Revisited*. 2012. International Conference on Financial Cryptography and Data Security, pp 129-147, [accessed 12.02.2025], https://www.researchgate.net/publication/228448040_Security_Audits_Revisited
4. Gérard P. Cachon, Martin A. Lariviere; *Supply Chain Coordination with Revenue-Sharing Contracts: Strengths and Limitations.*Management Science, Vol. 51, No. 1, Incentives and Coordination in Operations Management, Jan. 2005, pp, 30-44, [accessed 25.04.2025], http://www.jstor.org/stable/20110305
5. Austin Ebel, Debasis Mitra. *Economics and optimal investment policies of Attackers and Defenders in cybersecurity.* Journal of Cybersecurity, July 2024, [accessed 12.02.2025]; https://academic.oup.com/cybersecurity/article/10/1/tyae019/7900094
6. Alessandro Fedele, Cristian Roner; *Dangerous games: A literature review on cybersecurity investments*. Journal of Economic Surveys, published by John Wiley & Sons Ltd, 2022; [accessed 12.01.2025], https://onlinelibrary.wiley.com/doi/full/10.1111/joes.12456
7. B. Roy Frieden and Raymond J. Hawkins. *Asymmetric information and economics*. Physica A: Statistical Mechanics and its Applications, 389(2):287–295, 2010.
8. Lawrence A. Gordon and Martin P. Loeb. *The economics of information security investment*. In ACM Transactions on Information and System Security (TISSEC), Volume 5, Issue 4, pp 438-457, 2002, [accessed 02.04.2025], https://doi.org/10.1145/581271.581274
9. Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn, and Lei Zhou. *Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the gordon-loeb model.* Journal of Information Security, 06:24–30, 2015. [accessed 25.01.2025], https://www.researchgate.net/publication/273176128_Externalities_and_the_Magnitude_of_Cyber_Security_Underinvestment_by_Private_Sector_Firms_A_Modification_of_the_Gordon-Loeb_Model
10. Lawrence A. Gordon, Martin P. Loeb, *Investing in Cybersecurity: Insights from Gordon-Loeb Model,* Journal of Information Security, 07(02), 2016, pp 49-59, [accessed 12.04.2025], https://www.researchgate.net/publication/299408557_Investing_in_Cybersecurity_Insights_from_the_Gordon-Loeb_Model
11. Santjeev Goyal, Adrien Vigier, *Attack, Defence, and Contagion in Networks*, Review of Economic Studies, 2014, 81, pp 1518-1542, [accessed 23.01.2025], https://www.jstor.org/stable/43551742
12. Jens Grossklags, Nicholas Christin, *Secure or Insecure? A Game-Theoretic Analysis of Information Security Games*. Conference: Proceedings of the 17th International Conference on World Wide Wb, WWW 2008, Bejing, China, April 21-25, 2008, [accessed 23.02.2025], https://www.researchgate.net/publication/221022685_Secure_or_Insure_A_Game-Theoretic_Analysis_of_Information_Security_Games

13. Kjell Hausken. *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, 2006, [accessed: 25.01.2025], https://www.researchgate.net/publication/220198744_Returns_to_information_security_investment_The_effect_of_alternative_information_security_breach_functions_on_optimal_investment_and_sensitivity_to_vulnerability
14. C. Derrick Huang, Qing Hu, Ravi S. Behara; *An economic analysis of the optimal information security investment in the case of risk-averse firm*. International Journal of Production Economics, Volume 114, Issue 2, August 2008, [accessed 12.02.2025], https://www-sciencedirect-com.ezproxy.utlib.ut.ee/science/article/pii/S0925527308001199
15. C. Derrick Huang and Ravi S. Behara. *Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints.* International Journal of Production Economics, 141(1):255–268, 2013. [accessed 25.01.2025], https://www.sciencedirect.com/science/article/pii/S0925527312002678
16. ISO/IEC. *Information technology — security techniques — guidelines for cybersecurity*. 2012.
17. Shinichi Kamiya, Kang Jun-Koo, Kim Jungmin, Andreas Milidonis, René M. Stulz, *Risk management, firm reputation, and the impact of successful cyberattacks on target firms*. Journal of Financial Economics, Volume 139, Issue 3, March 2021, pp 719-749, [accessed 18.03.2025], https://www.sciencedirect.com/science/article/abs/pii/S0304405X20300143
18. Timothy R. Kayworth and Dwayne Whitten. *Effective information security requires a balance of social and technology factors*. MIS Q. Executive, 9, 2012.
19. Mazaher Kianpour, Stewart Kowalski, and Harald Øverby. *Systematically understanding cybersecurity economics: A survey*. Sustainability, 13, 12 2021. [accessed 12.04.2025], https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2978306
20. Kerry Krutilla, Alexander Alexeev, Eric Jardine, David Good. *The Benefits and Costs of Cybersecurity Risk Reduction: A Dynamic Extension of the Gordon and Loeb Model.* Risk Analysis. Volume 41, Issu 10, October 2021, pp 1795-1808, [accessed 23.02.2025],
21. https://onlinelibrary-wiley-com.ezproxy.utlib.ut.ee/doi/10.1111/risa.13713
22. Breden Kuerbis, Farzaneh Badiei. *Mapping the cybersecurity institutional landscape*. Digital Policy 2017. [accessed 18.04.2024], https://repository.gatech.edu/bitstreams/27f2da77-fa22-4968-ab07-dcced3395447/download
23. Howard Kunreuther, Geoffrey Heal. *Interdependent Security*. The Journal of Risk and Uncertainty, 26:2/3; pp 231-249, 2003, [accessed 25.02.2025], https://www.jstor.org/stable/41755017
24. Hau L. Lee, V. Padmaanabhan, Seungjin Whang; *Information Distortion in a Supply Chain: The Bullwhip Effect*. Management Science, Vol 50, No. 12, December 2004, pp 1875-1886; [accessed 25.04.2025], http://www.jstor.org/stable/30046159
25. Yuxin Li, Derek Bosworth. *R&D spillovers in a supply chain and productivity performance in British firms*. The Journal of Technology Transfer, Volume 45, pp 177-204, 2020, [accessed 8.04.2025], https://link.springer.com/article/10.1007/s10961-018-9652-x
26. Jon Randall Lindsay. *Restrained by design: the political economy of cybersecurity*. Digital Policy, Regulations and Governance, Volume 19 Issue 6, September 2017, [accessed 18.04.2025], https://www.emerald.com/insight/content/doi/10.1108/dprg-05-2017-0023/full/html
27. Tyler Moore. *The economics of cybersecurity: Principles and policy options*. International Journal of Critical Infrastructure Protection, 3(3):103–117, 2010.
28. Anna Nagurney, Patrizia Daniele, Shivani Shukla. *A supply chain network game theory model of cybersecurity investments with nonlinear budget constraints*. 29. April 2016, Annals of

Operational Research, Volume 248, pp 405-427, [accessed 22.03.2025], https://link.springer.com/article/10.1007/s10479-016-2209-1

29. Mahour Mellat Parast. *The impact of R&D investment on mitigating supply chain disruptions: Empirical evidence from U.S. firms*. International Journal of Production Economics, Volume 227, September 2020, [accessed 12.04.2025], https://www.sciencedirect.com/science/article/abs/pii/S0925527320300657
30. Christian Roner. *Three essays on the economics of cybersecurity.* 2022. Free University Bozen-Bolzano. PhD Thesis. [accessed 28.01.2025], https://bia.unibz.it/esploro/outputs/doctoral/Three-essays-on-the-economics-of/991006574298701241
31. Y. Shiozawa, K. Taniguchi, and M. Morioka. *Microfoundations of Evolutionary Economics*. Evolutionary Economics and Social Complexity Science. Springer Japan, 2016.
32. Henry R.K. Skeoch. *Expanding the gordon-loeb model to cyber-insurance*. Computers Security, 112:102533, 2022.
33. Gerry Smith, *Massive Target Hack Traced Back to Phishing Email.* HuffPost, Feb 12, 2014, [accessed 27.01.2025] https://www.huffpost.com/entry/target-hack_n_4775640
34. Georgios Spanos, Lefteris Angelis; *The impact of information security events to the stock market: A systemic literature review*. Computer & Security, Volume 58, May 2016, pp 216-229; [accessed 2.05.2025]; https://www.sciencedirect.com/science/article/pii/S0167404816300013
35. Hal Varian. *System Reliability and Free Riding*, Economics of Information Security. Advances in Information Security series, volume 12, pages 1–15. Springer US, Boston, MA, 2004. [accessed 12.01.2025], https://people.ischool.berkeley.edu/~hal/Papers/2004/reliability
36. Eva Weishäupl, Emrah Yasasin, and Guido Schryen. *Information security investments: An exploratory multiple case study on decision-making, evaluation and learning*. Computers Security, 77:807–823, 2018.
37. Willemson, Jan. *On the Gordon & Loeb Model for Information Security Investment*. 2006, [accessed 12.01.2025], https://www.researchgate.net/publication/244404155_On_the_GordonLoeb_Model_for_Information_Security_Investment
38. Willemson, Jan. *Extending the Gordon & Loeb Model for Information Security Investment.* Conference Paper. Cybernetica Ltd, Institute of Computer Science. University of Tartu. February 2010, [accessed 12.02.2025]; https://www.researchgate.net/publication/244404155_On_the_GordonLoeb_Model_for_Information_Security_Investment
39. Yong Wu, Gengzhong Feng, Nengmin Wang, Huigang Liang. *Game of information security investment: Impact of attack types and network vulnerability, Expert Systems with Applications*, Volume 42, Issues 15–16, 2015, [accessed 12.02.2025]; https://www.sciencedirect.com/science/article/pii/S0957417415002274

Appendix 1 – Nash equilibrium, perfect information

We will discuss the solution when we do have perfect information – firm *i* and firm *j* know how much other is investing. We have optimal cybersecurity investments equation (10) as follows:

$$z_i^* = \frac{(\alpha \cdot \beta \cdot v_i \cdot L_i)^{\frac{1}{\beta+1}} - 1}{\alpha} - \gamma z_j \quad (1a)$$

Then we apply this for both firms and get:

$$z_1 = \frac{(\alpha \cdot \beta \cdot v_1 \cdot L_1)^{\frac{1}{\beta+1}} - 1}{\alpha} - \gamma z_2 \quad (2a)$$

$$z_2 = \frac{(\alpha \cdot \beta \cdot v_2 \cdot L_2)^{\frac{1}{\beta+1}} - 1}{\alpha} - \gamma z_1 \quad (3a)$$

To find Nash equilibrium, we need to solve this system of equations. For this let introduce the following parameters:

$$A_1 = \frac{(\alpha \cdot \beta \cdot v_1 \cdot L_1)^{\frac{1}{\beta+1}} - 1}{\alpha} \quad (4a)$$

$$A_2 = \frac{(\alpha \cdot \beta \cdot v_2 \cdot L_2)^{\frac{1}{\beta+1}} - 1}{\alpha} \quad (5a)$$

So, we can rewrite the equations (2a) and (3a) as follows:

$$z_1 + \gamma z_2 = A_1 \quad (6a)$$

$$z_2 + \gamma z_1 = A_2 \quad (7a)$$

To solve this problem, lets multiply equation (6a) with γ and get:

$$\gamma z_1 + \gamma^2 z_2 = \gamma A_1 \quad (8a)$$

To find z_2 we need to subtract (8a) from (7a) and get:

$$(z_2 + \gamma z_1) - (\gamma z_1 + \gamma^2 z_2) = A_2 - \gamma A_1$$

$$(1 - \gamma^2) z_2 = A_2 - \gamma A_1$$

$$z_2^* = \frac{A_2 - \gamma A_1}{(1-\gamma^2)} \quad (9a)$$

Now substitute z_2 in equation (6a) we get:

$$z_1{}^* = A_1 - \gamma z_2{}^* = A_1 - \gamma \cdot \frac{A_2 - \gamma A_1}{(1-\gamma^2)} \quad (10a)$$

From equation (10a) and (9a)we find Nash equilibrium:

$$z_1^* = \frac{A_1 - \gamma A_2}{(1-\gamma^2)}$$

$$z_2^* = \frac{A_2 - \gamma A_1}{(1-\gamma^2)}$$

This result perfectly indicates the free-riding problem described in Varian (2004): Firm 1 will reduce its investments to 0 as Firm 2 starts to invest, relying fully on Firm 2's investments in cybersecurity.

Appendix 2 – Visualisation of extended GL model with learning dynamics