Economic Implications of Cyber Security: Analyzing Firms Investment Decision

Love Mbata

A Thesis

In the Department of

Economics

Presented in Partial Fulfillment of the Requirements

for the Degree of

Master of Arts

at Concordia University

Montréal, Québec, Canada

September 2024

CONCORDIA UNIVERSITY

School of Graduate Studies

This is to certify that the Thesis prepared

By: Love Mbata

Entitled: Economic Implications of Cyber Security: Analyzing Firms Investment Decision

and submitted in partial fulfillment of the requirements for the degree of

Master of Arts (Economics)

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final Examining Committee:

_____Examiner

Dr. Ming Li

_____Supervisor

Dr. Jan Victor Dee

Approved by: _____

Dr. Christian Sigouin

Graduate Program Director

Date: _____ _____

Dr. Pascale Sicotte, Dean

Faculty of Arts and Science

Abstract

Economic Implications of Cyber Security: Analyzing Firms Investment Decision

Love Mbata

In an era of increasing digitization and reliance on digital technologies, the economic implications of cybersecurity have become a critical concern for firms across various sectors. This thesis provides a review of the existing literature on firms' decisions to invest in cybersecurity. This study aims to provide insights into the factors driving firms to enhance their cybersecurity measures by analyzing the economic rationale behind cybersecurity investments. There is not a lot that has been done in this particular topic, this thesis, building on the existing literature aims to provide more knowledge.

The model in this thesis explores the decision of firms to invest in cybersecurity, considering factors such as substitutability of products (cybersecurity), consumer preferences for security, and the benefits of cybersecurity investments. Through a comprehensive review of the economics of cybersecurity investments, this thesis provides a better understanding of the economic motivations and implications behind firms' decisions to invest in cybersecurity in today's digital landscape.

Acknowledgements

I would like to Acknowledge and appreciate my thesis supervisor, Dr. Jan Victor Dee, who has been instrumental in making this research possible, encouraging me to go beyond my expectations and give my very best. I am grateful for his willingness to guide, instruct, and demonstrate patience throughout the course of this research.

I would also like to appreciate Dr. Christian Sigouin, the department of Economics graduate program director for his guidance and instruction in the course Research Methodology which made it possible for me to write this research.

I would like to also acknowledge Wisdom D'almeida, Stephen Mbata, Tayo Abimbola, Sidonie Ndambi and Onyenezido Ikechukwu for their support and encouragement throughout the period of this research, you all were amazing.

I would like to appreciate my beloved Parents Mr & Dr. Mrs Mbata Benedict, and my family for their constant prayers and care since the inception of this program, your confidence in me made it possible to constantly strive to do better. I would like to appreciate the entire DLBC Montreal, without your support, this achievement would not have been possible. To my fellow peers and colleagues, thank you for the many discussions, shared experiences, and constructive feedback. It has been a privilege to work alongside such talented and inspiring individuals. Finally, my utmost appreciation goes to God Almighty, for the strength, will and Grace given to me to accomplish this milestone in my life.

Contents

List of Figures

List of Tables

1 Introduction

In an increasingly digitized world, the importance of cybersecurity has never been more pronounced. With organisations across all sectors heavily reliant on digital technologies, protecting digital assets against cyber threats has become a pressing economic concern. The financial implications of cybersecurity extend beyond mere technological considerations, encompassing complex cost-benefit analyses and market forces that influence decision-making processes at both organisational and societal levels.

This research aims to delve into the economic implications of cybersecurity investments, particularly analysing the factors that drive firms to invest in cybersecurity measures. Sarker (2020) define cybersecurity as a set of technologies and processes to protect computers, networks, programs, and data from attack, damage, or unauthorised access. The rapid advancement of technology and its integration into every facet of business operations have led to significant shifts in how cybersecurity is managed.In recent years, cybersecurity has undergone massive transformations driven by innovations in computing and data science, mainly through machine learning (ML) and artificial intelligence (AI). These technologies play a crucial role in discovering insights from data, thus significantly altering the cybersecurity landscape. Leading a new scientific paradigm, data science offers enhanced capabilities for identifying and mitigating cyber threats.

Callen, Fang, and Hope (2018) show that the financial sector has undergone a profound digital transformation, making it more susceptible to cyber-attacks. The evolution of Financial Technology (FinTech) and Regulatory Technology (RegTech) has increased the risks of cyber threats due to the expanding digital data landscape. Hackers find the financial industry a lucrative target, thus making robust cybersecurity measures indispensable. Regulatory bodies focus more on ensuring financial institutions implement stringent cybersecurity protocols to safeguard against potential threats. This emphasis on regulatory compliance highlights the critical role of cybersecurity in protecting financial systems and maintaining the integrity of digital transactions.

Lehto (2022) provides a comprehensive overview of the increasing frequency and sophistication of cyber-attacks against critical infrastructure. In 2019, the U.S. experienced over 140 daily ransomware attacks targeting public, state, and local government healthcare providers, marking a 65% increase from the previous year. This alarming trend underscores the urgency for robust

cybersecurity measures.

Lehto notes that the technology sector became the most targeted industry for the first time, accounting for 25% of all attacks. This shift highlights the exponential growth of digital data generated and stored by organisations, necessitating robust cybersecurity measures to protect sensitive information from unauthorised access, theft, or manipulation.

Effective cybersecurity protocols are essential for ensuring the security and integrity of valuable digital assets. The model proposed in this research aims to shed light on the factors driving firms to invest in cybersecurity. By examining the economic rationale behind such investments, this study provides insights into how businesses can balance the costs and benefits of cybersecurity measures. Several factors influence the decision-making process, including market dynamics, regulatory requirements, and the potential financial impact of cyber-attacks. Understanding these factors is crucial for developing effective cybersecurity strategies that protect organisational assets and enhance economic stability.

Cybersecurity is vital in mitigating various cyber threats and attacks organisations face daily. These threats include malware, phishing, ransomware, and other forms of cybercrime. Implementing robust cybersecurity strategies is crucial for reducing the risk of security breaches and data compromises. By proactively addressing security vulnerabilities and implementing robust defense mechanisms, organisations can enhance their resilience to cyber-attacks and minimise the impact of security incidents on their operations. This proactive approach to cybersecurity is essential for maintaining business continuity and operational resilience.

Cybersecurity is fundamental for effective organisational risk management. Identifying and addressing potential security risks through comprehensive cybersecurity measures helps businesses protect their IT systems, networks, and data from cyber threats. This proactive risk management approach minimises vulnerabilities, strengthens security posture, and mitigates the potential impact of security breaches on operations and reputation. Compliance with cybersecurity regulations and standards is critical to maintaining data privacy, protecting customer information, and avoiding legal consequences related to data breaches.

Moreover, cybersecurity is integral to ensuring business continuity and operational resilience. By safeguarding IT systems and networks from cyber threats, organisations can minimise disruptions, maintain service availability, and protect their reputation in the event of a security incident.

Prioritising cybersecurity measures not only helps organisations protect their critical assets but also enables them to uphold their commitments to customers, stakeholders, and regulatory bodies. This fosters trust and confidence in their security practices, enhancing their competitive advantage in the market.

Bissell, LaSalle, and Dal Cin (2019) examine that the average number of security breaches grew by 11% from 130 in 2017 to 145 in 2018 per organization. Their research showed that the average cost of cybercrime for an organization increased from $1.4 million to $13 million. These costs include penalties, reputational damage, stock value reduction, compliance breaches, privacy violations, and operational disruptions.

The average number of security breaches per organization has been on the rise, underlining the urgency for robust cybersecurity measures to combat these threats effectively. Furthermore, cybersecurity investment is essential for protecting the confidentiality, integrity, and availability of information in complex environments where people, software, and services interact over the internet. By investing in cybersecurity, organizations can mitigate the risks posed by cyber threats and vulnerabilities, ensuring the security of their digital assets and services.

This research contributes to existing literature by introducing a theoretical approach to support investment decisions in cybersecurity by analyzing the effects various key parameters have on the optimal level of investment. This is an introduction to the overview of the implications of cybersecurity investment. A few key parameters would be analyzed in this research to shed more light on this topic.

The remainder of this paper is organized as follows; Section 2 is provides an overview of the literature review, showing the various research findings of authors regarding investment decisions; Section 3 highlights the model setup-emphasizing the calculations and derivations of the Monopolistic and Duopolistic Markets; Section 4 introduces the Model results and brief interpretations; Section 5 covers the conclusion, effects of parameters and potential extension of our model.

2 Literature Review

Cybersecurity has become a crucial aspect of modern economies, with digital transformation making firms vulnerable to a wide range of cyber threats. This literature review examines the economic

rationale behind cybersecurity investments, drawing from empirical studies and theoretical frameworks that explain firms' decision-making processes regarding cybersecurity expenditure. The focus is on understanding how firms make decisions to invest, based on some defined parameters.

Cybersecurity investments are often driven by the need to protect digital assets from cyber threats such as data breaches, ransomware, and intellectual property theft. According to Demigha and Larguet (2021), the increasing frequency and sophistication of cyber-attacks have compelled firms to allocate more resources to cybersecurity. They proposed a stochastic programming framework that highlights the financial implications of underinvesting in cybersecurity, showing that businesses face significant operational disruptions and financial losses when cyber defenses are inadequate.

Sarker (2020) emphasizes that the financial industry, in particular, is at also risk due to the rapid growth of financial technologies (FinTech). This sector's reliance on digital transactions makes it a prime target for hackers, leading to a growing emphasis on cybersecurity investment in both financial institutions and regulatory bodies such as Securities and Exchange Commission (SEC) – USA, and European Securities and Markets Authority (ESMA) – European Union. A study by Callen, Fang, and Hope (2018)on financial risk management demonstrates the importance of robust cybersecurity protocols in safeguarding the integrity of financial systems. Their work suggests that firms with strong cybersecurity measures benefit from reduced risk premiums and lower costs of capital.

Gordon, Loeb, and Zhou (2015) highlights the tendency of firms to underinvest in cybersecurity, despite its critical importance. Their research shows that companies integrating cybersecurity within their internal control systems are more likely to invest more in this area, mitigating financial risks associated with cyber breaches. This insight underscores the need for cybersecurity to be treated not merely as an IT function but as an integral component of corporate governance and risk management strategies.

2.1 Regulations on Cybersecurity and Costs

Regulatory frameworks play a significant role in shaping firms' cybersecurity investments. Compliance with cybersecurity regulations helps companies avoid legal consequences and maintain

consumer trust. The financial costs associated with non-compliance are high, with fines and reputational damage being just some of the potential consequences. Lehto (2022) documents the increasing sophistication of cyber-attacks on critical infrastructure in the U.S., emphasizing the growing necessity for comprehensive regulatory measures. In 2019 alone, over 140 daily ransomware attacks targeted U.S. public and healthcare sectors, illustrating the urgency of cybersecurity investments to protect national infrastructure and sensitive information.

Anderson et al. (2013) note that cybersecurity investments are not without cost, newer cybercrimes have lower direct costs but significantly higher indirect and defense costs. For instance, spam botnets earned $2.7 million, while global spam prevention efforts exceeded $1 billion, highlighting the inefficiency of cybercrime defense. These costs include penalties, reputational damage, stock value reductions, and operational disruptions.

Chronopoulos, Lambertides, and Lendewig (2017) argue that despite the high cost of cybersecurity breaches, many organizations still fail to conduct adequate cost-benefit analyses when making cybersecurity investment decisions. This lack of comprehensive risk assessments often leads to suboptimal investment levels in cybersecurity, leaving firms vulnerable to cyber threats.

Fedele and Caruso (2022) further explore the economic impact of cybercrime on global GDP. Their research shows that cybercrime costs the global economy between 0.6% and 0.8% of GDP annually, amounting to approximately $608 billion in 2016. This substantial economic cost underscores the need for firms to allocate sufficient resources to cybersecurity to mitigate the potential financial fallout from cyber-attacks.

In competitive markets, firms' decisions to invest in cybersecurity are influenced not only by consumer preferences but also by the actions of competitors. The duopolistic model of cybersecurity investment, illustrates how the quality of a competitor's cybersecurity measures can impact the demand for a firm's products. In markets where products are substitutes, the degree of substitutability plays a crucial role in determining firms' cybersecurity investment strategies.

The research in this area shows that when products are close substitutes, an increase in the quality of one firm's cybersecurity measures leads to a significant decrease in the demand for the competitor's products. Conversely, when products are less substitutable, the impact on demand is less pronounced. This dynamic compels firms in competitive markets to strategically invest in cybersecurity to maintain their market position and customer base.

Consumer demand for cybersecurity plays a pivotal role in shaping firms' investment strategies. In the monopolistic model, the lambda parameter represents the strength of consumer preferences for cybersecurity. Firms are more likely to invest in higher levels of cybersecurity when consumers place a high value on the security of their digital assets. This is supported by the findings of Hausken (2014), who suggests that firms can increase their market share and consumer loyalty by investing in robust cybersecurity measures that meet the growing demand for digital security.

In conclusion, the literature reviewed in this study provides valuable insights into the factors influencing firms' decisions to invest in cybersecurity. This review highlights the existing work on this, although not a lot has been done in this area, and there is a wide gap in terms of empirical work as there is not a lot of data to fully answer this question. This simple setup is a first step towards analyzing this problem and proposing a way forward in further research.

3 Model Setup

3.1 Monopolistic setup

The model begins with a simple monopolistic setup formulated from a standared linear demand curve with a benefit to investing and a cost of investing. The benefit of investing here for a general good is to obtain security. Firms are willing to provide the security that maximizes their profit, and consumers also prefer products that are more secure, and can gurantee the protection of their digital assets. The purpose of the firm's decision to invest is driven by profit maximization, achieved by choosing optimal quantities and levels of security, which is given by the equation below.

$$\pi(p, x_i, a, b, \lambda) = \mathbf{R}(p, x) - C(q) - I(x) \tag{1}$$

where π is the profit for the firm, and $C(Q)$ is the Cost for producing demand q, a, b, λ are the parameters, π is a function of both price and the level of security. $\mathbf{R}$ is the Revenue, which is a function of Price and level of security. I is the Investment cost which depends on the level of security x_i

The levels of cyber security in this model is noted as x_i, and the cost of investing in x_1 level of security is given by:

$$I(x) = \phi + \gamma x_i + \beta x_i^2 ... \tag{2}$$

The investment function here has a diminishing marginal return, Firms can achieve a low level of security relatively inexpensive but getting a higher level of security is very costly, hence the upward slope.

If $\lambda\ is = 0$ then consumers are not interested in the security of their goods or services, and would not be willing to pay for it. Consumer's utility depends on the quantity (or price) and the level of cybersecurity.

Consider a product i with quality (level of cyber security) x_i. Let the consumers's utility from consuming q_i units of products be given by:

$$u(q_i) = (a + \lambda x_i)q_i - \frac{q_i^2}{2} - P_i q_i \tag{3}$$

where P_i is the price of good i. Here, the parameter λ represents the consumer's preference for quality where higher values of λ means that consumers have a greater preference for quality. A consumer chooses the optimal quantity q_i to maximize her utility.

We have a simple demand function in a monopolistic setup below as:

$$\mathbf{Q} = a - bp + \lambda x \tag{4}$$

where

In the equation above, Q is quantity demanded, X_i is the level of cybersecurity. λ is the consumer's preference for security. (The higher the λ,the more the preference for cybersecurity) $\lambda \geq 0$. If λ is 0 then consumers don't care about cybersecurity. The optimal quantity q_i is defined by the following conditions.

$$\frac{\delta u}{\delta q_i} = a + \lambda x - q_i - P_i = 0 \tag{5}$$

which gives us the inverse demand function of good i

$$P_i = a + \lambda x - q_i \tag{6}$$

given the inverse demand function above, we can now write down a profit function for the firm i

$$\begin{aligned} \pi(q_i, X_i) &= (a + \lambda x_i - q_i)q_i - cq_i - I(x_i) \\ &= (a + \lambda x_i - q_i)q_i - cq_i - (\phi + \gamma x_i + \beta x_i^2) \end{aligned} \tag{7}$$

where c is the (constant) marginal cost of producing qi and $I(x_i) = \phi + \gamma x_i + \beta x_i^2$ is the cost of investing in x_i units of cybersecurity. For now, we assume that the cost of quality/cybersecurity is a fixed cost and does not affect the variable cost of producing good i.

3.2 Optimal Investment Levels

In obtaining the optimal levels of investment, we are assuming that it would be an interior solution. Taking first order conditions gives us:

$$\frac{\delta \pi}{\delta q_i} = a + \lambda x_i - 2q_i - c = 0 \Longrightarrow q_i = \frac{a + \lambda x_i - c}{2} \tag{8}$$

$$\frac{\delta \pi}{\delta x_i} = \lambda q_i - \gamma - 2\beta x_i = 0 \Longrightarrow x_i = \frac{\lambda q_i - \gamma}{2\beta} \tag{9}$$

Plugging equation (8) into (9) gives us the optimal level of investment x_i^* :

$$x_i^* = \frac{\lambda\left(\frac{a+\lambda X_i - c}{2}\right) - \gamma}{2\beta}$$

$$x_i^* = \frac{\lambda(a-c) - 2\gamma}{4\beta - \lambda^2} \tag{10}$$

From the equation (10) above It is evident that an increase in λ leads to a corresponding increase in the x_i^* ,The firm's optimal investment level is increasing in consumer's prefernce for cybersecurity.

Now we can solve for the optimal quantity q_i

$$q_i^* = \frac{a + \lambda\left(\frac{\lambda(a-c)-2\gamma}{4\beta\lambda^2}\right) - c}{2} \Longrightarrow \frac{2\beta(a-c) - \lambda\gamma}{4\beta - \lambda^2} \tag{11}$$

Note that if consumers do not value quality $(\lambda = 0)$ then equation (11) simplifies to $q_i^* = \frac{a-c}{2}$ which is the optimal monopoly quantity given an inverse demand function $P = a - Q$. Given q_i^* and x_i^* we can now solve for the optimal price

$$P_i^* = a + \lambda x_i^* - q_i^*$$

$$= a + \lambda\Big[\frac{\lambda(a-c) - 2\theta_1}{4\beta - \lambda^2}\Big] - \Big[\frac{2\beta(a-c) - \lambda\gamma}{4\theta - \lambda^2}\Big] \tag{12}$$

$$P_i^* = \frac{2\beta(a+c) - \lambda^2 c - \lambda\theta}{4\beta - \lambda^2} \tag{13}$$

Again, note that if consumers do not value cybersecurity $(\lambda = 0)$ then the optimal price is $P_i^* = \frac{a+c}{2}$ which is the optimal monopoly price.

3.3 Duopolistic Setup

In this section,we consider the case where there are two firms (1 and 2) competing in both quantity and quality, the following utility function is written for the duopolistic model.

3.3.1 Profit in competing Firms

The duopolistic setup is modeled similarly to the setup of Toshimitsu and Mori (2014). The utility derived from the consumption of these 2 goods is given as follows:

$$U\Big[q_1, q_2, x_1, x_2] = [\alpha(q_1 + q_2) - \frac{1}{2}(q_1^2 + q_2^2) - \theta q_1 q_2] + [(x_1 - \epsilon_2 x_2)q_1 \\ +(x_2 - \epsilon_1 x_1)q_2] - p_1 q_1 - p_2 q_2 \tag{14}$$

where p_1, p_2 is the price of good 1 and 2, repectively and q_1, q_2 is the quantity of good 1 and 2 repectively, and x_1, x_2 is the quality (level) of cybersecurity.We assume that the marginal utility of quality/cybersecurity is 1 per unit. The parameter epsilon represents the decrease in marginal utility as a result of a competing product having a higher level of cybersecurity. The Parameter θ in this model represents the degree of substitutability between products of both firms in this market.

The optimal Quantity for firm 1 is defined by the following conditions:

$$\frac{\delta U}{\delta q_1} = \alpha + x_1 - \epsilon x_2 - q_1 - \theta q_2 - p_1 = 0 \tag{15}$$

The inverse demand function of the good 1 is given below, $x_1 \geq 0$ and $x_2 \geq 0$

$$p_1 = \alpha + x_1 - \epsilon_2 x_2 - \theta q_2 - q_1 \tag{16}$$

For firm 2 in the duopolistic competition the optimal quantity for the firm 2 is defined by the following conditions:

$$\frac{\delta U}{\delta q_2} = \alpha + x_2 - \epsilon_1 x_1 - q_2 - \theta q_1 - p_2 = 0 \tag{17}$$

The inverse demand function is therefore given as:

$$p_2 = \alpha + x_2 - \epsilon_1 x_1 - \theta q_1 - q_2 \tag{18}$$

We can then solve the profit function for firm 1 and firm 2. The profit function for Firm 1 is given as

$$\Pi_1(q_1, x_1) = p_1 q_1 - c q_1 - I(x_1) = (\alpha + x_1 - \epsilon_2 x_2 - \theta q_2 - q_1) q_1 - c q_1 - (\phi + \gamma x_1 + \beta x_1^2) \tag{19}$$

where c is the (constant) marginal cost of producing qi and $I(x_1) = \phi + \gamma x_1 + \beta x_1^2$ is the cost of investing in x_1 units of cybersecurity. For now, we assume that the cost of quality/cybersecurity is fixed and does not affect the variable cost of producing good 1.

Taking first-order conditions gives us:

$$\frac{\delta \Pi_1}{\delta q_1} = \alpha + x_1 - \epsilon_2 x_2 - \theta q_2 - 2q_1 - c = 0 \Longrightarrow q_1 = \frac{\alpha + x_1 - \epsilon_2 x_2 - \theta q_2 - c}{2} \tag{20}$$

$$\frac{\delta \Pi_1}{\delta x_1} = q_1 - \gamma - 2\beta_2 x_1 = 0 \Longrightarrow x_1 = \frac{q_1 - \gamma}{2\beta} \tag{21}$$

The profit function for firm 2 is given as:

$$\begin{aligned} \Pi_2(q_2, x_2) = p_2 q_2 - c q_2 - I(x_2) \\ = (\alpha + x_2 - \epsilon_1 x_1 - \theta q_1 - q_2) q_2 - c q_2 - (\phi + \gamma x_2 + \beta x_2^2) \end{aligned} \tag{22}$$

Taking first-order conditions gives us:

$$\frac{\delta \Pi_2}{\delta q_2} = \alpha + x_2 - \epsilon_1 x_1 - \theta q_1 - 2q_2 - c = 0 \Longrightarrow q_2 = \frac{\alpha + x_2 - \epsilon_1 x_1 - \theta q_1 - c}{2} \tag{23}$$

$$\frac{\delta \Pi_2}{\delta x_2} = q_2 - \gamma - 2\theta_2 x_2 = 0 \Longrightarrow x_2 = \frac{q_2 - \gamma}{2\beta} \tag{24}$$

3.3.2 Best Response in competing firms

The both firms would choose the quantity of cybersercurity to provide for the consumers. Now plugging equation. (20) and (23) into (20) we would have:

$$\begin{aligned} q_1 = \frac{\alpha + [\frac{q_1 - \gamma}{2\beta}] - \epsilon_2 [\frac{q_2 - \gamma}{2\beta}] - \theta q_2 - c}{2} \\ 4\beta q_1 = 2\alpha\beta + q_1 - \gamma - \epsilon_2 [q_2 - \gamma] - 2\gamma\theta q_2 - 2\beta c \end{aligned} \tag{25}$$

Collecting like terms would give us:

$$4\beta q_1 - q_1 = 2\beta(\alpha - c) - \gamma_1(1 - \epsilon_2) - q_2(\epsilon_2 - 2\beta\theta) \tag{26}$$

$$
\begin{aligned}
q_1(4\beta - 1) &= 2\beta(\alpha - c) - \gamma(1 - \epsilon_2) - q_2(\epsilon - 2\beta\theta) \\
\frac{q_1(4\beta - 1)}{(4\beta - 1)} &= \frac{2\beta(\alpha - c) - \gamma(1 - \epsilon_2) - q_2(\epsilon_2 - 2\beta\theta)}{(4\beta - 1)}
\end{aligned} \tag{27}
$$

Then;

$$
q_1 = \frac{2\beta(\alpha - c) - \gamma(1 - \epsilon_2) - q_2(\epsilon_2 - 2\beta\theta)}{4\beta - 1} \tag{28}
$$

The quantity of cybersecurity provided by firm 2 can be calcuated as follows, pluging equation (23) and (20) into (22)

$$
\begin{aligned}
q_2 &= \frac{\alpha + [\frac{q_2 - \gamma}{2\beta}] - \epsilon_1[\frac{q_1 - \gamma}{2\beta}] - \theta q_1 - c}{2} \\
4\beta q_2 = 2\alpha\beta &= q_2 - \gamma - \epsilon_1[q_1 - \gamma] - 2\gamma\theta q_1 - 2\beta c
\end{aligned} \tag{29}
$$

Collecting like terms would give us:

$$
4\beta q_2 - q_2 = 2\beta(\alpha - c) - \gamma(1 - \epsilon_1) - q_1(\epsilon_1 - 2\beta\theta) \tag{30}
$$

$$
\begin{aligned}
q_2(4\beta - 1) &= 2\beta(\alpha - c) - \gamma(1 - \epsilon_1) - q_1(\epsilon - 1\beta\theta) \\
\frac{q_2(4\beta - 1)}{(4\beta - 1)} &= \frac{2\beta(\alpha - c) - \gamma(1 - \epsilon_1) - q_1(\epsilon_1 - 2\beta\theta)}{(4\beta - 1)}
\end{aligned} \tag{31}
$$

Then;

$$
q_2 = \frac{2\beta(\alpha - c) - \gamma(1 - \epsilon_1) - q_1(\epsilon_1 - 2\beta\theta)}{4\beta - 1} \tag{32}
$$

This shows the production level for Firm 2 in a competitive market where both firms are investing in cybersecurity, and their products are viewed as substitutes by consumers. The quantity produced by Firm 2 is influenced by its own production costs, the competition from Firm 1, and the

level of substitutability between the two firms' products. When cybersecurity investment becomes costly, or when Firm 1 produces more, Firm 2 reduces its own output to balance the competitive dynamics and maintain profitability.

3.3.3 Optimal Quantities and Investment Levels in Competing Firms

In a competitive market, firms must decide how much to produce to maximize their profits while considering the actions of their rivals. To obtain the optimal q_1^*, plugging Equation (31) into equation (27)

$$q_1 = \frac{2\beta(\alpha - c) - \gamma(1 - \epsilon_2) - \left[\frac{2\beta(\alpha-c)-(\gamma(1-\epsilon_1))-q_1(\epsilon_1-2\beta\theta)}{4\beta-1}\right](\epsilon_2 - 2\beta\theta)}{4\beta - 1} \tag{33}$$

Simplifying the equation

$$\begin{aligned} q_1(4\beta_2 - 1)^2 = (4\beta - 1)(2\beta(\alpha - c)) - (4\beta - 1)(\gamma(1 - \epsilon_2)) \\ -(\epsilon_2 - 2\beta\theta)(2\beta(\alpha - c)) + (\epsilon_2 - 2\beta\theta)(\gamma(1 - \epsilon_1) \\ +(\epsilon_2 - 2\beta\theta)(\epsilon_1 - 2\beta_2\theta)q_1 \end{aligned} \tag{34}$$

Then we have the equation below, during the process of simulating these to obtain optimality, we are considering a case where we have an interior solution. The values assigned to the each parameter is such that we would obtain a positive optimality.

$$q_1^* = \frac{2\beta(\alpha - c)[(4\beta - 1) - \epsilon_2 + 2\beta\theta] + \gamma\big[(\epsilon - 2\beta\theta)(1 - \epsilon_1) - (4\beta - 1)(1 - \epsilon_2)\big]}{\big[(4\beta - 1)^2 - (\epsilon_2 - 2\beta\theta)(\epsilon_1 - 2\beta\theta)\big]} \tag{35}$$

To obtain the Optimal Quantity for the firm 2:

$$q_2 = \frac{2\beta(\alpha - c) - \gamma(1 - \epsilon_1) - \left[\frac{2\beta(\alpha-c)-(\gamma(1-\epsilon_2))-q_2(\epsilon_2-2\beta\theta)}{4\beta-1}\right](\epsilon_1 - 2\beta\theta)}{4\beta - 1} \tag{36}$$

Simplifying the equation

$$q_2(4\beta-1)^2 = (4\beta-1)(2\beta_2(\alpha-c)) - (4\beta-1)(\gamma(1-\epsilon_1))$$
$$-(\epsilon_1-2\beta\theta)(2\beta(\alpha-c)) + (\epsilon_1-2\beta\theta)(\gamma(1-\epsilon_2) + (\epsilon_1-2\beta\theta)(\epsilon_2-2\beta\theta)q_2 \tag{37}$$

Then;

$$q_2^* = \frac{2\beta(\alpha-c)[(4\beta-1)-\epsilon_1+2\beta\theta] + \gamma\big[(\epsilon_1-2\beta\theta)(1-\epsilon_2) - (4\beta-1)(1-\epsilon_1)\big]}{\big[(4\beta-1)^2 - (\epsilon_1-2\beta\theta)(\epsilon_2-2\beta\theta)\big]} \tag{38}$$

Optimal Levels of Investment in Competing Firms

To obtain the optimal level of investment x_i*

$$x_1 = \frac{q_1-\gamma}{2\beta} \tag{39}$$

Plugging the optimal quantity for firm 1 obtaind in equation (43) into equation (50) would give;

$$x_1 = \frac{\left[\frac{2\beta(\alpha-c)[(4\beta-1)-\epsilon_2+2\beta\theta]+\gamma\left[(\epsilon_2-2\beta_2\theta)(1-\epsilon_1)-(4\beta-1)(1-\epsilon_2)\right]}{\left[(4\beta-1)^2-(\epsilon_2-2\beta\theta)(\epsilon_1-2\beta\theta)\right]}\right]-\gamma}{2\beta} \tag{40}$$

Further simplification:

$$x_1 = \frac{2\beta(\alpha-c)[(4\beta-1)-\epsilon_2+2\beta\theta] + \gamma\big[(\epsilon_2-2\beta\theta)(1-\epsilon_1) - (4\beta-1)(1-\epsilon_2)\big]}{\big[(4\beta-1)^2 - (\epsilon_2-2\beta\theta)(\epsilon_1-2\beta\theta)\big](2\beta)} \tag{41}$$

$$-\frac{\gamma\big[(4\beta-1)^2 - (\epsilon_2-2\beta\theta)(\epsilon_1-2\beta\theta)\big]}{\big[(4\beta-1)^2 - (\epsilon_2-2\beta\theta)(\epsilon_1-2\beta\theta)\big](2\beta)}$$

$$x_1^* = \frac{2\beta(\alpha-c)[(4\beta-1)-\epsilon_2+2\beta\theta] + \gamma\big[(\epsilon_2-2\beta\theta)(1-2\beta\theta) - (4\beta-1)(4\beta-\epsilon_2)\big]}{\big[(4\beta-1)^2 - (\epsilon_2-2\beta\theta)(\epsilon_1-2\beta\theta)\big](2\beta)} \tag{42}$$

The second firm has it's investment level given as follows:

$$x_2 = \frac{q_2-\gamma}{2\beta} \tag{43}$$

Plugging the optimal quantity for firm 2 obtaind in equation (49) into equation (55) would give;

$$x_2 = \frac{\left[\frac{2\beta(\alpha-c)[(4\beta-1)-\epsilon_1+2\beta\theta]+\gamma\left[(\epsilon_1-2\beta\theta)(1-\epsilon_2)-(4\beta-1)(1-\epsilon_1)\right]}{\left[(4\beta-1)^2-(\epsilon_1-2\beta\theta)(\epsilon_2-2\beta\theta)\right]}\right]-\gamma}{2\beta} \tag{44}$$

The optimal x_2^* is given as:

$$x_2 = \frac{2\beta(\alpha-c)[(4\beta-1)-\epsilon_1+2\beta\theta]+\gamma\left[(\epsilon_1-2\beta\theta)(1-\epsilon_2)-(4\beta-1)(1-\epsilon_1)\right]}{\left[(4\beta-1)^2-(\epsilon_1-2\beta\theta)(\epsilon_2-2\beta\theta)\right](2\beta)} \tag{45}$$

$$-\frac{\gamma_1\left[(4\beta-1)^2-(\epsilon_1-2\beta\theta)(\epsilon_2-2\beta\theta)\right]}{\left[(4\beta-1)^2-(\epsilon_1-2\beta\theta)(\epsilon_2-2\beta\theta)\right](2\beta)}$$

$$x_2^* = \frac{2\beta(\alpha-c)[(4\beta-1)-\epsilon_1+2\beta\theta]+\gamma\left[(\epsilon_1-2\beta\theta)(1-2\beta\theta)-(4\beta-1)(4\beta-\epsilon_1)\right]}{\left[(4\beta-1)^2-(\epsilon_1-2\beta\theta)(\epsilon_2-2\beta\theta)\right](2\beta)} \tag{46}$$

The equation 41 and 45 above represent the optimal levels of cybersecurity investment for two competing firms in a duopolistic market. Both equations show that a firm's investment decision is influenced by its own cybersecurity costs, the substitutability of its product with that of its competitor, and the cross-effects of the competitor's cybersecurity investment on consumer demand. A higher cost of investment leads to lower cybersecurity spending, while greater substitutability between the firms' products intensifies competition, forcing both firms to adjust their investments strategically.

3.4 Discussion of Model Assumptions

We assume that consumers's preference for quality determines the optimal investment of firms and this applies to all the levels of investment the firms chooses to carry out. As Toshimitsu and Mori (2014) assumes that upgrading the quality leads to increased demand, we assume that consumers who are more inclined to cybersecurity would demand more if the quality of security they get is better.

We assume that consumers' preferences for cybersecurity are identical. In the monopolistic model, the marginal utility of quality is λ for each consumer. In the duopolistic setup consumers have a marginal utility of $q_i - \epsilon_i q_j$ which means that we assume $\lambda = 1$

Similar to the model of Toshimitsu and Mori (2014), consumers gain more benefit from cybersecurity the more assets they have. The consumers in this model are risk neutral.

4 Model Results

We solve this model by first setting up a monopolistic market where only one firm offers the good (cybersecurity) in the market and consumers choose how many units to purchase based on the level of cybersecurity. Firms in this model choose the optimal level of cybersecurity in order to maximize profit. The quantity of cybersecurity provided by the firm in this market is dependant on the price placed on a unit of cybersecurity and the preference for cybersecurity.

There is an investment cost $I(x_i) = \phi_\theta + \gamma x_i + \beta x_i^2$ that progressively increases as the level of security increases. The profit derieved in the monopolistic market is a function of the price, quantity, investment level, and preferences. This can be seen in equation 4.

The competitive market has a more complicated setup, here we have two firms in the market that produce similar goods with varying levels of cybersecurity. The cost of Investment in cybersecurity remains the same as in the monopolistic setting. It increases as the security level increases. In this market we aim to derive the optimal investment level for the firm that would ensure equilibrium, as well as the optimal quantity demanded that would ensure the firms make the right investment decision.

The following Propositions solidifies these results

4.1 Model Results for the Monopolistic setup

Proposition 1 (Firms optimal level of investment in a monopolistic market) *Consider a monopolistic market with identical consumers. Suppose that consumers have a preference λ for cybersecurity and the cost of cyber security is given by $I(X) = \phi_\theta + \gamma x_i + \beta x_i^2$, the optimal level of cybersecurity is given by:*

$$x_i^* = \frac{\lambda(a-c) - 2\gamma_1}{4\beta - \lambda^2} \tag{47}$$

Moreover, we can see that the optimal level of investment is increasing in λ and decreasing in γ andβ. This means that firms invest more when consumers have a greater preference for cybersecurity and less as the cost of cybersecurity increases.

Proposition 2 (Optimal quantity and in a Monopolistic Market) *Consider a monopolistic market with identical consumers. Suppose that the firms choose the quantity of security to provide and the price for security they provide The optimal quantity as derieved earlier in this research is stated as:*

$$q_i^* = \frac{2\beta(a-c) - \lambda\gamma}{4\beta - \lambda_2}$$

Note that if $\lambda = 0$ then the optimal monopoly quantity simplifies to $q_i^* = \frac{a-c}{2}$ and the optimal price is also given as: $p_i^* = \frac{a+c}{2}$ if $\lambda = 0$.

The firms therefore choose the optimal quantity that would guarantee the most profit for them. The firm must consider the price elasticity of demand for its product or service. If demand is relatively inelastic (meaning consumers are less sensitive to price changes), the firm can increase prices without significantly affecting sales volume. Conversely, if demand is elastic, a price increase might lead to a substantial drop in sales.

4.2 Model Results for the Duopolistic setup

Proposition 3 (Competing Firms optimal level of investment) *Similar to the monopolistic market, consider a duopolistic market with identical consumer. Suppose that consumers have a preference for cybersecurity λ but in this model setup it is $= 1$, then the optimal level of investment is given by*

$$x_1^* = \frac{2\beta(\alpha-c)[(4\beta-1) - \epsilon_2 + 2\beta\theta] + \gamma\big[(\epsilon_2 - 2\beta\theta)(1-2\beta\theta) - (4\beta-1)(4\beta-\epsilon_2)\big]}{\big[(4\beta-1)^2 - (\epsilon_2 - 2\beta\theta)(\epsilon_1 - 2\beta\theta)\big](2\beta)} \tag{48}$$

This gives us the optimal level of investment for Firm 1 which is dependent on the various parameters, and a increase or decrease in the parameters aftects the level of investment in either of

the firms. This is symmetric to the other firm in the market. This does not show the parameters affect the optimal level of investment, hence the need for the simulations to depict how each key variable affects the level of investment.

Proposition 4 (Competing Firms choice of optimal quantity) *In a duopolistic market, where two firms compete by offering products with varying levels of cybersecurity, the optimal quantity of security is a function of the various parameters also. The firms produce at the optimal quantities whaile maximizing their profit. This also shows how much the firm sells.*

There is an interdependence of parameters in obtaining the optimal Quantity for the firm 1, although its not obvious from the optimal quantity provided by firm one shown below,

$$q_1^* = \frac{2\beta(\alpha - c)[(4\beta - 1) - \epsilon_2 + 2\beta\theta] + \gamma\big[(\epsilon_2 - 2\beta\theta)(1 - \epsilon_1) - (4\beta - 1)(1 - \epsilon_2)\big]}{\big[(4\beta - 1)^2 - (\epsilon_2 - 2\beta\theta)(\epsilon_1 - 2\beta\theta)\big]} \tag{49}$$

The optimal quantity of the second firm is given as:

$$q_2^* = \frac{2\beta(\alpha - c)[(4\beta - 1) - \epsilon_1 + 2\beta\theta] + \gamma\big[(\epsilon_1 - 2\beta\theta)(1 - \epsilon_2) - (4\beta - 1)(1 - \epsilon_1)\big]}{\big[(4\beta - 1)^2 - (\epsilon_1 - 2\beta\theta)(\epsilon_2 - 2\beta\theta)\big]} \tag{50}$$

We assume firms have similar products (cybersecurity) thereby creating a competitive environment. The decision made by the one firm affects the other firm. Each firm must consider the actions and strategies of its competitor when making pricing and investment decisions.

4.3 Impact of Parameters on Level of Investment

In the Monopolistic setup of this research, there are two parameters of interest, that is the λ and the γ and they both play significant roles in this Market. In the Duopolistic setup two additional parameters are introduced which have an effect on the level of investment in cybersecurity, they are the ϵ and the θ parameters. The λ parameter measures the consumers preference for cybersecurity in both of the markets. A higher value for λ indicates that the consumer has a stronger preference for the product. and this can be seen as a willingness to pay the price for that amount of security. This parameter also indicates the level to which the firm would choose to invest in cybersecurity. In the competitive market λ is assummed to be 1, that is $\lambda = 1$ for the consumers in the market

The γ parameters in the models represents the investment cost incurred by firms for providing cybersecurity. It captures the increasing cost of enhancing security, with higher levels of cybersecurity requiring significantly more investment. The investment function reflects diminishing returns, meaning that the cost rises steeply as the firm provides higher levels of security.

The (ϵ) parameters measures how changes in the quality of one firm's product affect the demand for the competing firm's product in a duopolistic setup. A higher ϵ indicates that consumers shift more quickly to the higher-quality product when one firm improves its cybersecurity. Conversely, a lower ϵ suggests that consumers are less sensitive to changes in security quality between the competing firms. In summary, each parameter reflects how much a firm's cybersecurity investment is influenced by competition and ϵ_1, applies to Firm 1 and ϵ_2 applies to Firm 2. Essentially, both parameters capture the firms' sensitivity to competitive pressures related to cybersecurity.

The θ represents the degree of substitutability between the products of two competing firms. In the duopolistic market, a higher value of θ means the products are close substitutes, so an increase in the security quality or price of one product will have a significant effect on the demand for the other product. Conversely, a lower θ implies less substitution between the products, making the firms' investments in cybersecurity more independent of each other.

5 Model Interpretation

In this section we are looking at the effect a change in ϵ would have on the optimal level of investment for both firms, this would be symetrical as both firms share similar characteristics. For the Firm 1 where we have the optimal investment noted as follows:

$$x_1^* = \frac{2\beta(\alpha - c)[(4\beta - 1) - \epsilon_2 + 2\beta\theta] + \gamma\big[(\epsilon_2 - 2\beta\theta)(1 - 2\beta\theta) - (4\beta - 1)(4\beta - \epsilon_2)\big]}{\big[(4\beta - 1)^2 - (\epsilon_2 - 2\beta\theta)(\epsilon_1 - 2\beta\theta)\big](2\beta)} \tag{51}$$

we would be conducting simulations to asses the changes with an increase or decrease in ϵ_1. This same applies to the second firm in this model, simulation on the key parameters would be conducted to asses their effect on the optimal levels of investment. The second firm has the optimal

investment level given as:

$$x_2^* = \frac{2\beta(\alpha - c)[(4\beta - 1) - \epsilon_1 + 2\beta\theta] + \gamma\big[(\epsilon_1 - 2\beta\theta)(1 - 2\beta\theta) - (4\beta - 1)(4\beta - \epsilon_1)\big]}{\big[(4\beta - 1)^2 - (\epsilon_1 - 2\beta\theta)(\epsilon_2 - 2\beta\theta)\big](2\beta)} \quad (52)$$

Both firms aim to maximize their profit, which is derived from the consumption of their products and the quality (level) of cybersecurity they provide. This utility is influenced by the quantity sold and the quality of the product. In the Duopolistic setup, all of the parameters remain the same and have the same effect but the λ Parameter, in the duopolistic model we assume it is $\lambda = 1$.

For the simulations seen below, we set α to 10, and Cost (c) to 5, the ϵ_1, ϵ_2 between [0,1], the γ parameters [0,4], the θ parameter also is set between [0,1]. The graphs below illustrate how the optimal levels change as we change the various parameter values.

The graph indicates values of substitutability and various levels of investment, there is a significant increase in investment as substitutabillity slightly increases.

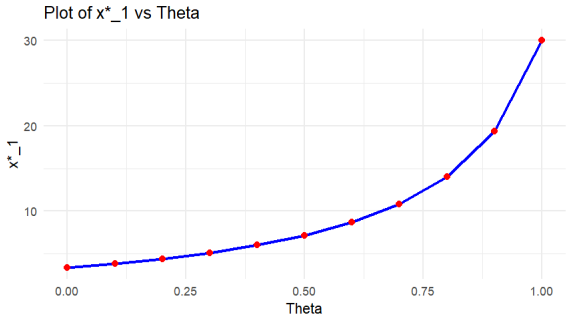
At θ = 0 there is substitutability, and investment is about 3.33, the optimal investment is zero, indicating no incentive for firms to invest when there is no competition from substitutes. As θ increases (higher substitutability), the investment increases also.

This trend demonstrates that as competition intensifies (as θ increases), firms are willing to invest more in cybersecurity. However, there is a sharp rise as θ moves toward 1.0, which represents extreme competition, where firms invest heavily to stand out from competitors.

The Figure 1 graph implies that if products are a closer substitutes there is more incentive to invest in cybersecurity because the only differentiator is that one product is more secured than the other. For example if in the market there are two products with similar charcteristics, what would make consumers interested in one over the other would be the added advantage of security one has over the other. If the products are very different, it wouldn't matter if firms invest in it as consumers wouldn't really care about it, or make a choice of one over the other.

In summary, Table 1 quantifies the effect of increasing product substitutability on cybersecurity investments. The trend shows that with rising θ, firms invest more in cybersecurity, peaking at very high levels of substitutability. As can be seen in the table shown below when θ = 1 the level of investment in cybersecurity goes up to 30.0, giving an upward inclination, which is quite an increment from the intial 3.33 when there is little or no substitutability.

Figure 1: Variation of x_1^* with θ



Note: The graph above illustrates the changes in the level of investment with varying levels of θ

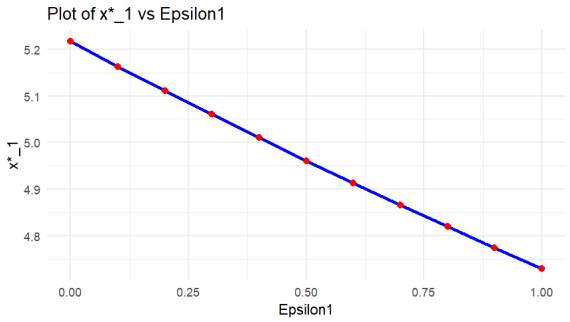
Table 1: Results of Parameter Sensitivity Analysis on x_1^* with θ

$\gamma = 2$	$\beta = 0.5$	$\epsilon_1 = 0.2$	$\epsilon_2 = 0.2$	$C = 2$	$\alpha = 10$
θ			x_1^*		
0.0			3.33		
0.2			4.40		
0.4			6.00		
0.6			8.66		
0.8			14.00		
1.0			30.00		

Figure 2 illustrates the relationship between ϵ_1 and x_1^*. This shows how the optimal investment in cybersecurity, denoted as x_1^*, varies with the parameter ϵ_1. This parameter represents a competitive sensitivity factor, or how a firm reacts to competition based on consumers' security preferences. As the parameter ϵ_1 increases, the level of optimal investment decreases sharply. This decline in investment discourages excessive cybersecurity investment, as firms may see diminishing returns on such investments when consumer preferences or competitive pressures intensify.

The figure shows that, when ϵ_1 is low, firms have higher incentives to invest in cybersecurity. However, as ϵ_1 increases, the firm's motivation to continue investing diminishes, reflecting this with the values. This indicates a strong negative correlation between $\epsilon_1$and x_1^*. It also suggests that firms will reduce their cybersecurity expenditure as the influence of external factors such as competitor quality or the cost of additional investments becomes more pronounced. The relationship depicted in Table 2 reinforces this point, as the firm's optimal investment level decreases with rising ϵ_1. The drop in investment from 5.22 at ϵ_1 =0.0 to 4.73 units at ϵ_1= 1.0 reflects how firms react to changes

Figure 2: Variation of x_1^* with ϵ_1



Note: The graph above illlustrates the changes in the level of investment with varying levels of ϵ_1

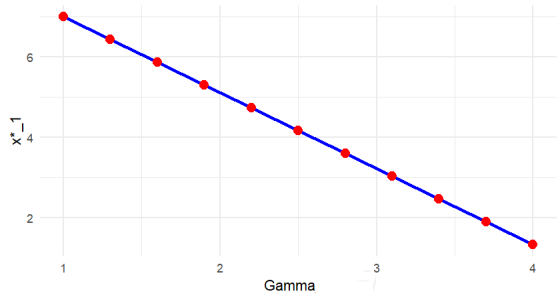
Table 2: Results of Parameter Sensitivity Analysis on x_1^* with ϵ_1

$\gamma = 2$	$\beta = 0.2$	$\theta_1 = 0.3$	$\epsilon_2 = 0.2$	$C = 2$	$\alpha = 10$
ϵ_1			x_1^*		
0.0			5.22		
0.2			5.11		
0.4			5.00		
0.6			4.91		
0.8			4.82		
1.0			4.73		

in consumer preferences and the competitive landscape. In cybersecurity investment terms, firms will only invest heavily when they expect that consumers value their security offerings more than the competition.

Figure 3 illustrates the variation of the optimal investment level x_1^* as a function of the parameter γ_1, which represents the investment cost for cybersecurity. As γ, increases, the optimal investment x_1^* decreases. This reflects the fact that higher costs associated with cybersecurity investment lead to a reduction in the amount firms are willing to invest in security measures. The graph shows a linear decrease in investment as we increase the values of γ. This indicates that as the cost of investing in cybersecurity grows, firms become increasingly cautious about how much they allocate toward cybersecurity, and eventually, they invest less because the return on investment diminishes. The results in Figure 3 and Table 3 demonstrate a fundamental concept in cybersecurity investment: as costs increase, firms become less inclined to invest heavily in security. This is a natural response to higher costs, as firms need to balance their security needs with their overall

Figure 3: Variation of x_1^* with γ



Note: The graph above illlustrates the changes in the level of investment with varying levels of γ

Table 3: Results of Parameter Sensitivity Analysis on x_1^* with γ

$\theta = 0.3$	$\beta = 0.5$	$\epsilon_1 = 0.2$	$\epsilon_2 = 0.2$	$C = 2$	$\alpha = 10$
γ_1			x_1^*		
1.0			7.00		
1.6			5.87		
2.2			4.73		
2.8			3.60		
3.4			2.47		
4.0			1.33		

profitability. If the cost of implementing additional cybersecurity measures becomes prohibitively high, the firm's optimal investment will decrease, as reflected by the declining trend in Figure 3.

6 Conclusion

The comprehensive analysis of the economic implications of cybersecurity and firms' investment decisions reveals critical insights into the complex dynamics driving these investments. In an era marked by escalating cyber threats and increasing reliance on digital technologies, firms must navigate a multifaceted landscape to safeguard their digital assets effectively. This study emphasizes the significant influence of consumer preferences on cybersecurity investments and explores how other variables affect investment levels.

The various relationships indicates that heightened consumer awareness and preference for security can significantly shape firms' strategic decisions regarding cybersecurity expenditures. To determine optimal investment levels, firms must consider various factors, including preference of

Consumers, Quality of Competing firms goods, and the substitutability of their products. This approach ensures that firms can make informed decisions that balance investment costs with the anticipated benefits of reduced cyber risk, offering a promising outlook for the future.

The study employs a dual model setup, "monopolistic and duopolistic", to provide an understanding of how different parameters impact firms' cybersecurity investment decisions. In a monopolistic market, consumer preference for security directly influences the firm's investment in cybersecurity. Conversely, the duopolistic model illustrates that competition between firms further complicates these decisions, as each firm's investment levels affect the other's strategies and outcomes. The empirical evidence and theoretical models presented in the literature review support the study's findings. The increasing financial impact of cybercrime on firms and the global economy underscores the urgent need for robust cybersecurity measures.

The integration of cybersecurity into firms' internal control systems and adoption of information-sharing practices are highlighted as potential drivers for increased cybersecurity investments. This underinvestment is a serious concern, especially since private firms own a significant portion of critical infrastructure. The study underscores the need for firms to conduct comprehensive cost-benefit analyses and cyber risk assessments to determine the optimal investment required for cybersecurity measures. The findings suggest that a more informed and strategic approach to cybersecurity investments can help firms mitigate risks and enhance their security posture.

Furthermore, drawing from the research conducted by Toshimitsu and Mori (2014) the research shows that firms must balance cybersecurity costs, consumer demand, and the competitive pressure exerted by substitutability between products. It also demonstrates how firms adjust their cybersecurity spending based on the cost of investment and the degree to which their competitors' cybersecurity affects their own market position Ultimately, this research provides significant insights into the economic implications of cybersecurity and the factors influencing firms' investment decisions.

As the digital landscape evolves, ongoing research and adaptive strategies will be essential to address the dynamic challenges of cyber threats. By prioritising cybersecurity investments, firms can safeguard their critical assets, fulfil their commitments to stakeholders, and build trust and confidence in their security practices.

7 Acknowledgment of Generative AI and AI-assisted tools

During the preparation of my thesis, I used ChatGPT to review my analysis, and help organize my research by fixing gramatical errors effectively. After using this tool I reviewed and edited the content as needed and take full responsibility for the content of my thesis.

References

Anderson, Ross, Chris Barton, Rainer Böhme, Richard Clayton, Michel JG Van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. 2013. "Measuring the cost of cybercrime." *The economics of information security and privacy,* 265–300.

Bissell, Kelly, Ron LaSalle, and Paolo Dal Cin. 2019. *The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study.* Accenture Security.

Callen, Jeffrey R., Xiaohui Fang, and Ole-Kristian Hope. 2018. "Corporate Risk Management and the Cost of Equity Capital." *Journal of Financial Economics* 128 (3): 585–607.

Chronopoulos, Dimitrios, Neophytos Lambertides, and Alexander Lendewig. 2017. "Cybersecurity and Firm Performance: Evidence from the Introduction of the GDPR in Europe." *European Financial Management* 24 (5): 793–813.

Demigha, Oualid, and Ramzi Larguet. 2021. "Hardware-based solutions for trusted cloud computing." *Computers & Security* 103:102117.

Fedele, Marco, and Andrea Caruso. 2022. "Blockchain Technology for Cybersecurity: An Overview." *Future Internet* 14 (2): 42.

Gordon, Lawrence A., Martin P. Loeb, and Lei Zhou. 2015. "The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?" *Journal of Computer Security* 23 (1): 1–27.

Hausken, Kjell. 2014. "Returns to information security investment: Endogenizing the expected loss." *Information Systems Frontiers* 16:329–336.

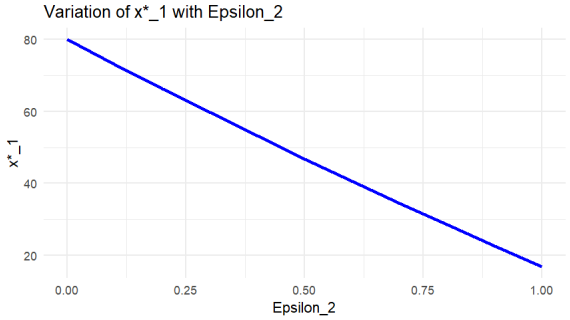
Lehto, Martti. 2022. "Cybersecurity Education and Research: Trends and Best Practices." *Journal of Cybersecurity and Privacy* 2 (1): 47–65.

Sarker, Iqbal H. 2020. "Cybersecurity Data Science: An Overview from Machine Learning Perspective." *Journal of Defense Modeling and Simulation* 17 (3): 207–227.

Toshimitsu, Masaaki, and Kohei Mori. 2014. "The Impact of Information Security Incidents on the Market Value of Firms in Japan." *Pacific-Basin Finance Journal* 29:92–114.

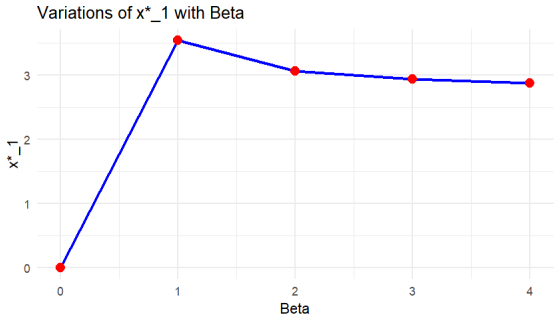
8 Appendix A: Figures

Figure 4: Variation of x_1^* with ϵ_2



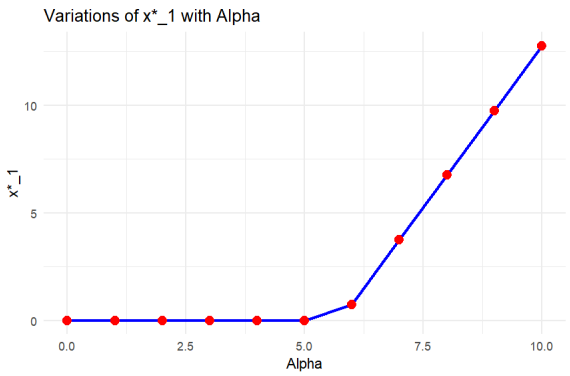
Note: The graph above illlustrates the changes in the level of investment with varying levels of ϵ_2

Figure 5: Variation of x_1^* with β



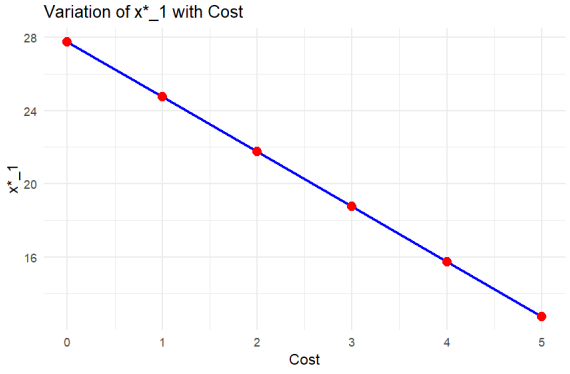
Note: The graph above illlustrates the changes in the level of investment with varying levels of β

Figure 6: Variation of x_1^* with α



Note: The graph above illlustrates the changes in the level of investment with varying levels of α_1

Figure 7: Variation of x_1^* with $Cost$



Note: The graph above illlustrates the changes in the level of investment with varying levels of $Cost$

9 Appendix B: Tables

Table 4: Results of Parameter Sensitivity Analysis on x_1^* with ϵ_2

$\gamma = 2$	$\beta = 0.5$	$\epsilon_1 = 0.2$	$\theta = 0.3$	$C = 2$	$\alpha = 10$
ϵ_1			x_1^*		
0			80		
0.5			0		
1.0			0		
1.5			0		
2.0			0		

Table 5: Results of Parameter Sensitivity Analysis on x_1^* with β

$\theta = 0.3$	$\gamma = 2$	$\epsilon_1 = 0.2$	$\epsilon_2 = 0.2$	$C = 2$	$\alpha = 10$
ϵ_1			x_1^*		
0.0			80.0		
0.2			66.30		
0.4			53.20		
0.6			40.30		
0.8			27.80		
1.0			15.70		

Table 6: Results of Parameter Sensitivity Analysis on x_1^* with α

$\theta = 2$	$\beta = 0.5$	$\epsilon_1 = 0.2$	$\epsilon_2 = 0.2$	$C = 2$	$\alpha = 10$
ϵ_1			x_1^*		
0.0			0		
2.5			0		
5.0			0		
7.5			5.25		
10			2.75		

Table 7: Results of Parameter Sensitivity Analysis on x_1^* with $Cost$

$\theta = 0.3$	$\beta_2 = 0.5$	$\epsilon_1 = 0.2$	$\epsilon_2 = 0.2$	$C = 2$	$\alpha = 10$
ϵ_1			x_1^*		
0.0			27.75		
1			24.75		
2			21.75		
3			18.75		
4			15.75		
5			12.75		

9.1 Additional Calculations

Alternatively, we can solve for the optimal price directly. From equation (6), we can obtain the demand function $q_i = a - P_i + \lambda X_i$ and the corresponding profit function

$$\pi(P_i, X_i) = P_i q_i - c q_i - I(X_i)$$
$$= P_i(a - P_i + \lambda x_i) - c(a - P_i + \lambda x_i) - (\gamma_0 + \gamma_1 x_i + \beta_2 x_i^2)$$

Taking derivatives gives us the first-order conditions

$$\frac{\delta \pi}{\delta P_i} = a - 2P_i + \lambda X_i + c = 0 \Longrightarrow P_i = \frac{a + \lambda X_i + c}{2}$$

$$\frac{\delta \pi}{\delta X_i} = \lambda(P_i - c) - \gamma - 2\beta_2 X_i \Longrightarrow X_i = \frac{\lambda(P_i - c) - \gamma}{2\beta}$$

Substituting equation (14) into (15) gives the optimal investment level X_i^*.

$$X_i^* = \frac{\lambda\Big(\big[\frac{a+\lambda X_i + c}{2}\big] - c) - \gamma}{2\theta_2}$$
$$X_i^* = \frac{\lambda(a-c) - 2\theta_1}{4\beta - \lambda^2}$$

Substituting X^* back into equation (14) we can find the optimal price

$$P_i^* = \frac{a + \lambda\left[\frac{\lambda(a-c)-2\gamma}{4\beta_2-\lambda^2}\right] + c}{2}$$
$$P_i^* = \frac{2\beta(a+c) - \lambda^2 c - \lambda\gamma_1}{4\beta - \lambda^2}$$

Both methods would give the same optimal prices and qualities.

Calculations for the optimal quantities Collecting like terms

$$q_1(4\beta-1)^2 - q_1(\epsilon_1 - 2\beta\theta)(\epsilon_2 - 2\beta\theta) = 2\beta(\alpha - c)\big[(4\beta-1) - (\epsilon_2 - 2\beta\theta)\big] + \gamma\big[(\epsilon_2 - 2\beta\theta)(1-\epsilon_1) - (4\beta-1)(1-\epsilon_2)\big]$$

Factorizing q_1 to obtain q_1^*

$$q_1\big[(4\beta-1)^2 - (\epsilon_2 - 2\beta\theta)(\epsilon_1 - 2\beta\theta)\big]$$
$$= 2\beta(\alpha - c)[(4\beta-1) - \epsilon_2 + 2\beta\theta] + \gamma\big[(\epsilon_2 - 2\beta\theta)(1-\epsilon_1) - (4\beta-1)(1-\epsilon_2)\big]$$

$$\frac{q_1\big[(4\beta-1)^2 - (\epsilon_2 - 2\beta\theta)(\epsilon_1 - 2\beta\theta)\big]}{\big[(4\beta-1)^2 - (\epsilon_2 - 2\beta\theta)(\epsilon_1 - 2\beta\theta)\big]}$$
$$= \frac{2\beta(\alpha - c)[(4\beta-1) - \epsilon_2 + 2\beta\theta] + \gamma\big[(\epsilon_2 - 2\beta\theta)(1-\epsilon_1) - (4\beta-1)(1-\epsilon_2)\big]}{\big[(4\beta-1)^2 - (\epsilon_2 - 2\beta\theta)(\epsilon_1 - 2\beta\theta)\big]}$$

$$q_1^* = \frac{2\beta(\alpha - c)[(4\beta-1) - \epsilon_2 + 2\beta\theta] + \gamma\big[(\epsilon_2 - 2\beta\theta)(1-\epsilon_1) - (4\beta-1)(1-\epsilon_2)\big]}{\big[(4\beta-1)^2 - (\epsilon_2 - 2\beta\theta)(\epsilon_1 - 2\beta\theta)\big]} \tag{53}$$

The calculation breakdown to obtain q_2^*

Collecting like terms

$$q_2(4\beta-1)^2 - q_2(\epsilon_1 - 2\beta\theta)(\epsilon_2 - 2\beta\theta) = 2\beta(\alpha - c)\big[(4\beta-1) - (\epsilon_1 - 2\beta\theta)\big] + \gamma\big[(\epsilon_1 - 2\beta\theta)(1-\epsilon_2) - (4\beta-1)(1-\epsilon_1)\big]$$

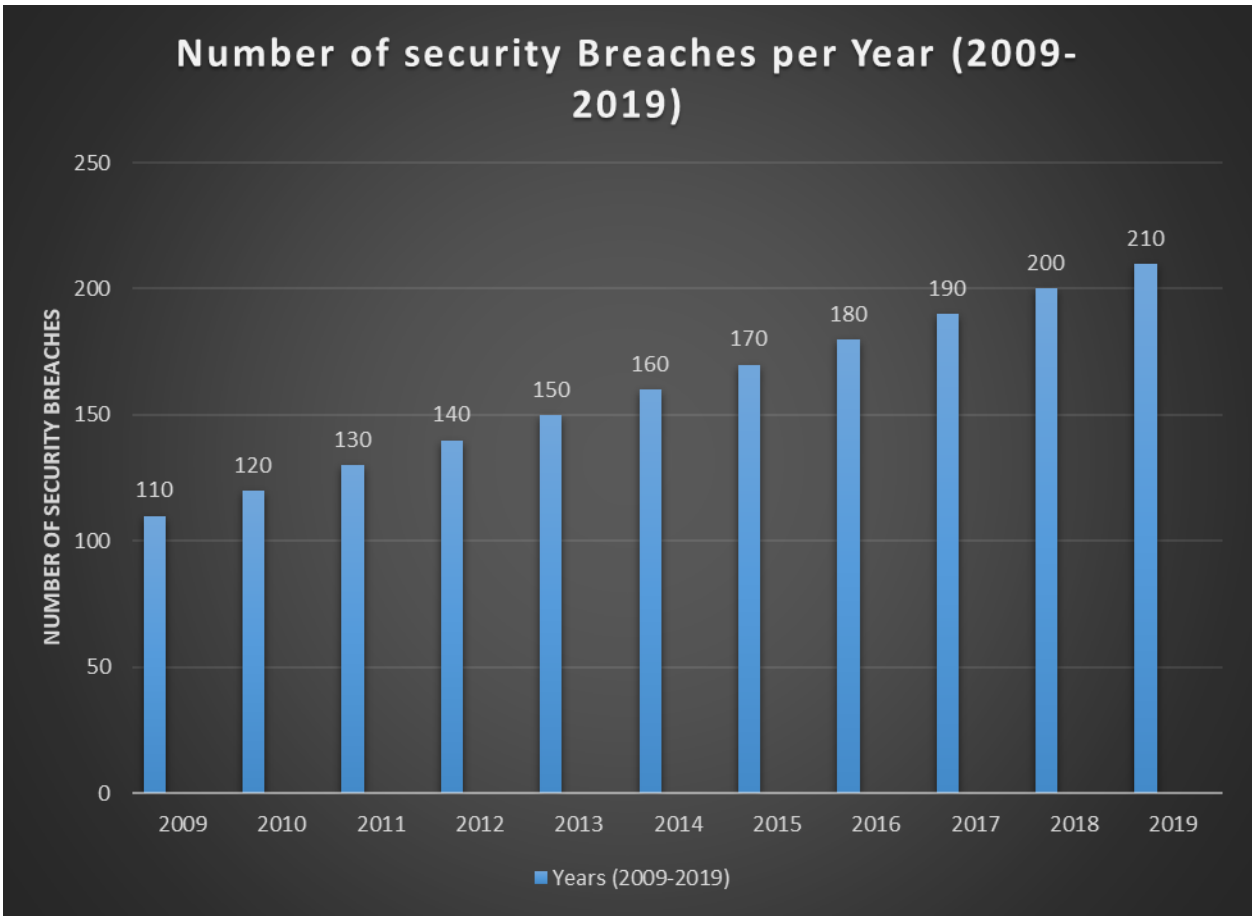
Factorizing q_2 to obtain q_2^*

$$q_2\big[(4\beta-1)^2-(\epsilon_1-2\beta\theta)(\epsilon_2-2\beta\theta)\big]$$
$$=2\beta(\alpha-c)[(4\beta-1)-\epsilon_1+2\beta\theta]+\gamma\big[(\epsilon_1-2\beta\theta)(1-\epsilon_2)-(4\beta-1)(1-\epsilon_1\big]$$

$$\frac{q_2\big[(4\beta-1)^2-(\epsilon_1-2\beta\theta)(\epsilon_2-2\beta\theta)\big]}{\big[(4\beta-1)^2-(\epsilon_1-2\beta\theta)(\epsilon_2-2\beta\theta)\big]}$$
$$=\frac{2\beta(\alpha-c)[(4\beta-1)-\epsilon_1+2\beta\theta]+\gamma\big[(\epsilon_1-2\beta\theta)(1-\epsilon_2)-(4\beta-1)(1-\epsilon_1)\big]}{\big[(4\beta-1)^2-(\epsilon_1-2\beta\theta)(\epsilon_2-2\beta\theta)\big]}$$

$$q_2^*=\frac{2\beta(\alpha-c)[(4\beta-1)-\epsilon_1+2\beta\theta]+\gamma\big[(\epsilon_1-2\beta\theta)(1-\epsilon_2)-(4\beta-1)(1-\epsilon_1)\big]}{\big[(4\beta-1)^2-(\epsilon_1-2\beta\theta)(\epsilon_2-2\beta_2\theta)\big]} \tag{54}$$

Figure 8: Number of Security Breaches per Year



Note: The graph above illlustrates the total amount of security breaches per year for a span of ten years.