VILNIUS UNIVERSITY BUSINESS SCHOOL
SUSTAINABLE CORPORATE FINANCE AND INVESTMENTS PROGRAMME

Rūta Okulič Kazarinaitė

THE FINAL MASTERS THESIS

Kibernetinio saugumo rizikų valdymas įmonių finansuose: poveikis investicijoms ir kapitalo kainai	**Cybersecurity risk management in corporate finance: impact on investments and cost of capital**

Student _____
(signature)

Supervisor _____
(signature)

_____
Assoc. Prof. Dr. Ieva Bužienė

Vilnius, 2025

SUMMARY

VILNIUS UNIVERSITY BUSINESS SCHOOL

SUSTAINABLE CORPORATE FINANCE AND INVESTMENTS STUDY PROGRAMME

RŪTA OKULIČ KAZARINAITĖ

CYBERSECURITY RISK MANAGEMENT IN CORPORATE FINANCE: IMPACT ON INVESTMENTS AND COST OF CAPITAL

Supervisor – Assoc. Prof. Dr. Ieva Bužienė

Master's thesis was prepared in Vilnius, in 2025

Scope of Master's thesis (project) – 57 pages.

Number of tables used in the FMTP - 18 pcs.

Number of bibliography and references - 118 pcs.

The masters thesis analyses cybersecurity risk management in the context of corporate finance, focusing on the impact on investment decisions and cost of capital.

The research problem: How do companies cybersecurity risk management and communication after a cyber incident shape investor and market reactions to the incidents?

The aim of this thesis is to explore how cybersecurity risk management and cyber incidents impact market reactions, investment behavior and perceived cost of capital.

The objectives set to achieve this objective are: to review and synthesize literature, to develop a methodology, to apply selected methods on a selected sample, and to interpret the results and provide conclusions and recommendations.

Research methods used in the thesis are the analysis of scientific literature, event study methodology, using a market model, qualitative assessment of corporate disclosures, and cross-sectional analysis to evaluate differences by incident characteristics.

Research results show no statistically significant aggregate market reaction to cybersecurity incidents. Cross-sectional analysis shows heterogeneity between sectors and response types across the sample. Firm communication and remediation practices do not mitigate short term valuation effects.

The main conclusion of the thesis is that cybersecurity incidents do not generate strong short term market reactions on average, but reveal differences in how risk is perceived across firms and incidents. Cybersecurity risk management appears to affect firm value mainly through long term mechanisms and not immediate market responses.

SANTRAUKA

VILNIAUS UNIVERSITETO VERSLO MOKYKLA
TVARŪS VERSLO FINANSAI IR INVESTICIJOS PROGRAMA
RŪTA OKULIČ KAZARINAITĖ

KIBERNETINIO SAUGUMO RIZIKŲ VALDYMAS ĮMONIŲ FINANSUOSE: POVEIKIS INVESTICIJOMS IR KAPITALO KAINAI

Darbo vadovas – Assoc. Prof. Dr. Ieva Bužienė
Darbas parengtas – 2025 m. Vilniuje
Darbo apimtis – 57 puslapiai
Lentelių skaičius darbe - 18 vnt.
Literatūros ir šaltinių skaičius - 118 vnt.

Magistro darbe analizuojamas kibernetinio saugumo rizikos valdymas įmonių finansų kontekste, daugiausia dėmesio skiriant jo poveikiui investiciniams sprendimams ir kapitalo kainai.

Tyrimo problema: Kaip įmonių kibernetinio saugumo valdymas ir komunikacija po kibernetinių incindentų formuoja investuotojų ir rinkos reakcijas į juos?

Tyrimo tikslas: atskleisti, kaip kibernetinio saugumo rizikos valdymas ir kibernetiniai incidentai veikia investicinį elgesį, rinkos reakcijas, ir kapitalo kainą.

Šiam tikslui pasiekti iškelti uždaviniai: apžvelgti ir susisteminti mokslinę literatūrą, sukurti tyrimo metodologiją, pritaikyti pasirinktus metodus pasirinktai incidentų imčiai bei interpretuoti gautus rezultatus ir pateikti išvadas bei rekomendacijas.

Darbe taikyti tyrimo metodai: mokslinės literatūros analizė, įvykių analizės (event study) metodas taikant rinkos modelį, įmonių viešųjų pranešimų kokybinis vertinimas ir analizė, skirta įvertinti skirtumus pagal incidentų charakteristikas.

Tyrimo rezultatai rodo, kad agreguotu lygmeniu kibernetinio saugumo incidentai nesukelia statistiškai reikšmingų rinkos reakcijų. Tarpsektorinė analizė atskleidžia skirtumus tarp sektorių ir reakcijų tipų imties viduje. Įmonių komunikacijos ir atsako būdas nešvelnina trumpalaikio poveikio įmonių vertei.

Pagrindinė darbo išvada: kibernetinio saugumo incidentai vidutiniškai nesukelia stiprių trumpalaikių rinkos reakcijų, tačiau atskleidžia skirtumus, kaip rizika vertinama skirtingose įmonėse ir incidentų atvejais. Kibernetinio saugumo rizikos valdymas labiau veikia įmonių vertę per ilgalaikius mechanizmus, bet ne tiesiogiai per rinkos reakcijas.

TABLE OF CONTENTS

LIST OF TABLES

INTRODUCTION

Cybersecurity risk has become an important factor in corporate decision making and financial markets. Digitalization of business processes, data-driven operations and interconnected supply chains have increased companies' exposure to cyber threats across industries. Cybersecurity incidents can impact businesses ranging from technical disruptions to disturbing operations, imposing reputational damage, regulatory challenges, legal costs and long term uncertainty. As a result,cybersecurity risk has evolved into an important component that needs to be covered in the context of corporate risk management, governance and investment strategy.

Cybersecurity incidents raise questions related to companies value, investment behaviour and perceived risk, and for this reason inventors, creditors and regulators increasingly treat cybersecurity as a part of a broader enterprise risk management, together with financial, operational and regulatory risks. Regulations such as GDPR, NIS2, DORA and others reinforce the financial relevance of cyber risk by linking disclosure, governance oversight and compliance costs to corporate reporting.

Despite this growing relevance, empirical evidence on how cybersecurity incidents affect firm value are wide ranged. Several studies document negative short term market reactions after major breaches, others find limited or insignificant effects. Existing research also shows substantial differences in market responses depending on incident characteristics, suggesting that cybersecurity incidents cannot be treated as homogeneous events and that investor reactions may depend on how incidents are framed, communicated and managed by the companies. This suggests that cybersecurity incidents cannot be treated as homogenous events and that all investor reactions may depend on how incidents are perceived, disclosed and managed by the affected firms.

The companies are also increasing the engagement with the public, communicating the cyber incidents. They disclose the events to reassure stakeholders, show control over the incidents and in attempts to control reputational damage. The stakeholders expect the companies to cover the incidents, and pay attention to timing of the announcement, accuracy and consistency. Companies are expected to provide sufficient information about their operations, costs of the incident, what actions were taken for remediation. Informing stakeholders on what risks might affect them is also important and expected. Researchers cover this area, analyzing how communication and strategy of disclosures mitigate market reactions or change investment behavior. For these reasons, disclosure requirements are also an important

study direction, because they can improve transparency and point to previously unobserved risks.

The research question: How do companies cybersecurity risk management and communication after a cyber incident shape investor and market reactions to the incidents?

The aim of this thesis is to explore how cybersecurity risk management and cyber incidents impact market reactions, investment behavior and perceived cost of capital. In order to achieve this aim, the objectives are set:

- Review and synthesise the academic literature on cybersecurity risk management, corporate finance and the effects of cyber incidents on investments and cost of capital.
- Develop a combined qualitative and quantitative methodology to investigate stock market reactions to cybersecurity incidents and to assess company level risk management and communication practices.
- Apply the developed methodology to a sample of cybersecurity incidents in publicly listed companies.
- Interpret the empirical results in the context of corporate finance theory and cybersecurity governance, provide conclusions and practical recommendations, including those for future research.

The research of the thesis applies a mixed methods approach. Theoretical foundation is established by performing a systematic analysis on existing research. After that, a quantitative analysis is carried out using an event study methodology based on the market model, that estimates abnormal returns and cumulative abnormal returns around cybersecurity incident disclosure dates. Then, statistical testing is applied to assess significance and cross-sectional variation. Qualitative analysis is based on a structured review of different kinds of corporate statements on the cyber events that are analyzed. That includes press releases, investor communications and annual reports and other files. Company responses then are assessed across predefined categories related to timing, remediation, investment, governance and communication. These qualitative categories then are linked to market outcomes, by comparing cumulative abnormal returns across response groups. The integration of quantitative and qualitative methods allows for more comprehensive interpretation of results.

The thesis is split into three parts. The first part covers theoretical literature on cybersecurity risk management, corporate governance and market reactions. The second part of the thesis presents the research methodology and data. The third part is empirical research results, including event study findings, cross-sectional analysis, qualitative assessment of

companies responses to cyber events and synthesis of the results. The thesis is finalized with conclusions, limitations and recommendations, including future research advice.

Novelty of the research comes from multiple aspects. The study uses combined qualitative and quantitative methodology that connect cybersecurity incident response to abnormal. This lets company communication and risk management frameworks to be evaluated with market reactions, aside from descriptive analysis. The study methods are integrating company level disclosure quality and response strength into classic cybersecurity event study methods. The methods also include cross-sectional market reaction analysis. The research is performed for a geographically underresearched market, focusing on publicly listed companies in Nordic Europe, Baltic countries and Poland. It is a region that is high in digitalization, has strong cybersecurity regulation frameworks and cybersecurity maturity, but limited evidence on what market reactions to cyber incidents are.

The research does have some limitations, because the empirical analysis is based on a relatively small sample of publicly reported cybersecurity incidents in the defined region in Europe. A small sample limits the statistical power of tests and the scope of the results.The study also relies on publicly available disclosures from multiple companies, all of which have different characteristics, vary in depth and transparency. The disclosures may not fully display internal risk management practices or financial impacts. Another limitation is that short term event windows are used to analyze immediate reactions of the cyber events, and long term changes are not evaluated.

The scientific value of the thesis extends existing cybersecurity event study literature by integrating company response behaviour into market reaction analysis. The practical value provides insights for managers, investors and regulators on how cybersecurity incidents are perceived in capital markets and how current disclosure and risk management practices may influence financial outcomes.

1. THEORETICAL REVIEW

The following chapter will provide a theoretical overview and existing empirical research related to cybersecurity risk in corporate finance. The chapter focuses on analyzing how cyber risk is managed by companies, how financing decisions for cybersecurity are made, what market reactions are to cyber risk and incidents, and what is the role of governance and regulation in this context. Table 1 systemizes core concepts covered in literature on cybersecurity risk management, including theoretical approach, empirical findings and insights relevant to the thesis.

Table 1 summarizes the dominant academic findings across five key thematic areas covered later in this chapter. Each of the following subsections (1.1 to 1.5) expands on these elements in greater detail.

Summary of theoretical concepts, models and insights on cybersecurity risk and corporate finance

Table 1

Summary of theoretical concepts, models and insights on cybersecurity risk and corporate finance

Topic	Concepts	Core Findings	Insights	Key Sources
Cybersecurity as a Financial Risk	ERM, systemic risk, cyber resilience; Governance Theory	Cybersecurity risk is increasingly recognized as a strategic and financial threat, with implications for reputation, operational continuity, and firm value.	Should be treated as a financial driver, not just technical vulnerability.	Stine et al. (2020); Mizrak (2023); Gale et al. (2022); Cheng et al. (2024)
Market Reactions to Breaches	Abnormal returns, Event Study Models, Reputation Score Models	Empirical studies demonstrate that cybersecurity breaches typically lead to negative abnormal stock returns and long-term reputational damage.	Need to connect valuation to financing conditions.	Day & Booker (2024); Huygen & Beulen (2025); Tosun (2021); Rushing et al. (2025); Zadeh et al. (2023)
Cost of Capital & Cyber Risk	Cost of equity/debt, information asymmetry; Agency Theory	Cybersecurity disclosure and governance influence the cost of capital by reducing information asymmetry and perceived risk.	Cyber governance should be part of credit risk analysis.	Florackis et al. (2022); Havakhor et al. (2021); Malliouris (2021); Jamilov et al. (2023); Choi et al. (2025)

Continuation of Table 1

Strategic Investment & Frameworks	Cyber investment as part of strategic investment; NIST, Adaptive Frameworks	Cybersecurity investment is treated as a strategic capital allocation decision, with frameworks guiding risk informed budgeting and planning.	Frameworks can be used to prioritize and justify cyber investments.	Fedele & Roner (2022); Mizrak (2023); Lee (2021); Ganin et al. (2020); Benton & Radziwill (2017)
Regulation & Governance	Compliance and disclosure; GDPR, NIS2, DORA, CSRD; ESG integration frameworks	Regulatory frameworks enhance cybersecurity governance, promote transparency, and contribute to improved stakeholder trust and financial performance.	Disclosure acts as a financial signal to investors.	Balboni & Francis (2025), Boggini (2024); Joswig & Kurz (2025); Kiesow Cortez & Dekker (2022); Clausmeier (2022); Liu & Shao (2025)

Source: Compiled by the author.

The following sections of this chapter flow from the topics covered in Table 1, and provide a base for the methodology and empirical research. The covered topics also motivate the formulation of hypotheses.

1.1 Cybersecurity as a financial risk factor

With the increasing digitality of the world and dependence on technology, there is a growing importance for companies to protect customers' data, operational continuity of their business and reputation. For this reason, cybersecurity in corporate finance has emerged as one of critical topics of research. Ensuring proper cybersecurity measures is necessary to keep the communities functioning properly. The World Economic Forum (2025) states that cybercrime has been persistently evolving, including more sophisticated and far-reaching attacks that require coordination from law enforcement and cybersecurity experts. These growing cyber events have the power to halt operations, undermine confidence in critical infrastructures and damage operational technology. Recent findings from Singh et al. (2025) cover the topic of cybersecurity resilience, and show how it is necessary in order to support innovation and long-term business performance, protecting valuable data and information systems within companies. They describe how having proactive policies for cybersecurity management forces companies to detect issues and find root causes which drives innovation, compared to simply responding to cyber events that delay these innovations. Cybersecurity has become a very

important topic in enterprise risk management, especially for companies in industries that deal with personal information or critical infrastructures. According to Lee (2021), cyber incidents can cause companies multiple financial costs including penalties, reputational harm, stock price decreases, and even while it is difficult to measure benefits and costs of investment in cyber risk management, it is essential for companies to stay current with the changes in cybersecurity, and respond to it accordingly.

Cybersecurity is also important for strategic and economic reasons. Cheng et al. (2024) study shows that cybersecurity has a significant positive impact on digital finance and is important for economic development. It analyzes GDP per capita and investment in network infrastructure that is shown to improve overall functionality of the services of digital finance.

Kiesow Cortez & Dekker (2022) covers risk management practices in the financial sector from the perspective of corporate governance theories. They point out that oftentimes companies underinvest in prevention of cyber incidents, and instead frame the incidents as unavoidable risk. At the same time they point out how reporting practices in the US and EU contexts are increasingly acknowledging data protection and privacy risk factors.

Cybersecurity risks affect interconnected company networks. Fotis (2024) explains how cyberattacks can point out companies' weak points by disrupting supply chains, and identify short and long term economic impacts on the company. The cyberattacks can restrain innovation and disrupt the supply chain, increasing the costs and reducing companies operational abilities. This shows how disruptions in one point of a network can impact others, increasing the risk of reputational damage. The paper also shows that incident response planning and cyber insurance both increase companies' recovery time and lower financial losses or expenses.

Cybersecurity is also a critical component of Enterprise Risk Management (ERM) because organizations increasingly recognize the strategic importance of it. Cybersecurity's integration into ERM Frameworks is important for business continuity, financial stability and organizational resilience. According to Stine et al. (2020), ERM involving cybersecurity now allows organizations to "identify, assess, and manage cybersecurity risk in the same context as other types of business risk". This ensures that cyber threats are evaluated and considered together with financial, operational and reputation risks. The study also highlights how the senior leaders within the company have a responsibility to holistically manage the risks, including those of cybersecurity, and how risk tolerance and appetite are set. This points to an understanding by companies that good cybersecurity requires planning, evaluation, influencing capital allocation, governance and company value. Some researchers analyze how apologies from senior level

management can impact investors' opinions positively, while stating that cybersecurity risk management strategies will be improved, without an official apology from a CEO yielding a lowest interest of investing for investors (Demek & Kaplan, 2023). The study also states that while some cybersecurity risks can be addressed, it does not eliminate the risk completely.

In certain industries, cyber incidents can very quickly damage a company' s reputation. A study by Saveljeva et al. (2025) describes how cybersecurity, when integrated to sustainable development, supports strategic resilience and organizational sustainability. They point out how cybersecurity is a fundamental element that together with ESG frameworks can reduce certain risks by implementing stronger disclosure, higher stakeholder trust and this way supports long term sustainable development of the enterprise. With cyber threats evolving, integrating cybersecurity to ERM or ESG frameworks is a way to protect companies' long term value. Cyber resilience is also named as a foundational element for both sustainability and recovery. According to Mizrak (2023) findings, cybersecurity should be integrated into risk management to protect data and improve resilience during cyber incidents. The study also states that cybersecurity should be recognized as a shared responsibility between companies' departments, and for successful integration of it, communication and financing are necessary. For these reasons, digital resilience of firms needs to be prioritized.

Yet, according to Gale et al. (2022), boards of directors often fail to provide effective cybersecurity oversight, because reporting is too technical and lacks structure. They point out that there still exists a disconnect between IT departments and the board, the reason for this being lack of technical knowledge on cybersecurity. Some directors avoid addressing the issue to avoid reputational damage or rely on one person with the most knowledge. Also covered by the authors is the idea on how regulations push companies to meet the needs, but does not put the focus on prevention. This leads to compromised cybersecurity and digital resilience decision making.

To summarize, the literature shows how cybersecurity cannot be looked at as a technical issue only, and has deeper and longer lasting effects on the company. Initial costs and issues from a cyber event can be solved quicker and with less financial strain with a strong ERM frameworks, but regulatory penalties, reputational damage, decline in stock prices are some of the long term hits a company needs to address. For this reason, integrating cybersecurity to enterprise risk management is needed to maintain the operational abilities of the company, to maintain shareholder trust and mitigate risks, especially in the long term. This leads to the discussion on how markets react to cybersecurity incidents and adjust capital allocation decisions in the following chapter.

1.2 Market Reactions to Cybersecurity Incidents and Corporate Valuation

How organizations manage cybersecurity risks can be analyzed by looking at financial markets. Investor sentiment and stock price reactions provide a certain signal of how the market perceives a company's preparedness or ability to manage and recover from cyber incidents. After the announcement of a cyber event, a reaction from the market is expected. By looking at the financial markets, these reactions or consequences of a cyber event can be measured. Research that analyzes the impact of cyber events on stock prices, consistently show that cyber incidents are followed by negative abnormal stock returns, in some cases elevated market volatility and other long-term reputational damages that might influence investor decision making (Day & Booker, 2024, Huygen & Beulen, 2025, Zadeh et al. ,2023). As summarized in Table 1, this area of research provides more quantifiable proof on how cyber incidents are connected to a company's value. This is especially true in industries that handle sensitive data, or rely on digital infrastructure. As cyber incidents are becoming more common, investors learn to incorporate cyber security resilience or management into risk assessments.

Companies, to remain competitive, have to keep up with the digitalization. Because of this, research on what market reactions are to cyber incidents has also grown. The research is important because it shows how investors price cyber risk and how it is incorporated into companies' evaluation. Some studies perform event analyses, most of them either calculating short term stock price reactions, or long term reactions that examine reputation, disclosure practices. Markets can react differently based on industry, breach type and regulations. For these reasons the existing research can provide context and justify hypotheses, variables and methods used further in the analysis.

Day & Booker (2024) employ a case study approach and examine incidents involving Equifax, Capital One, T-Mobile, Facebook, Google and others. Event study methods and statistical tests show significant stock price declines relative to the market after the incidents are announced. The study shows how investors' reactions are quick and negative, backing up the idea that markets view cyber incidents as a serious risk to the company. The study also displays that the visibility and not the size solely of the breach can produce stronger negative effects in the company’s reputational damage depending on the company’s industry. They highlight the need for clear communication and effective crisis management to mitigate the market reactions, stock price and investor confidence. Investment into advanced security technologies are recommended to the large corporations by the study.

A study by Huygen and Beulen (2025) based on 405 cyber events from 295 U.S. public companies, provides evidence on how short and long term market reactions differ according to breach type. They analyze the events based on categorization into exploitative, disruptive, and mixed events, where exploitative and mixed breaches trigger the strongest declines. The authors hypothesise if there are different reactions to the breaches if the company has been hit first-time or multiple times, with the findings not show significant devaluations in subsequent incidents, suggesting that investors might adjust expectations after the first-time event. The findings of the study also indicate that cybersecurity incidents can lower firm value in the long run as well as in short run in exploitative and mixed events, and prove that market reactions are different according to breach characteristics. They emphasize that investments into cybersecurity risk management are a better alternative in terms of long term reputation and stakeholder trust, than increased risk of cyber events that would come with financial impacts beyond the immediate direct costs.

Tosun (2021) analyzes the market response (short and long term) of 58 major corporate security breaches in the U.S. between 2004 and 2019. The results of the study show that for short term analysis, excess returns drop the day after the announcement, but traded volume and liquidity significantly increase the day of the announcement and could be attributed to increased attention of investors. The long term analysis shows that companies are not significantly affected within 5 years, but they incorporate cybersecurity into their policies, research and development or management. The study provides proof of negative shocks on the companies stock price and reputation short term, and long term changes due to a breach are not visible in the same ways, but rather a change in CEO or strategy or spending.

Long term effects of cyber events are also analyzed by researchers. Reputation Impact Score, introduced by Rushing et al. (2025), is a quantifiable framework to measure reputational damage by combining financial data with investor and customer sentiment. The paper analyzes specific cases like Equifax and SolarWinds, showing that long term reputational harm persists long after the initial market reaction, and can be more influential than financial harm in shaping opinion on the company post breach. The paper shows how transparency, efforts to repair reputation and relationships with stakeholders are all important factors in maintaining resilience after cyber incidents.

Another aspect in research is analyzing financial markets reaction based on certain cybersecurity breach disclosure laws. Cao et al. (2024) study the effect of U.S. data breach notification (DBN) laws, and based on a large dataset of 3600 companies between years 1997 and 2019. Their findings show a positive relation between DBN laws and negative stock price

reactions, noting that corporate governance and information asymmetry within other factors can influence the extent of the stock price reactions. This indicates how regulation that is aiming to improve transparency raises investors' awareness about breaches, but also concerns about companies' vulnerability and can lead to increased risk in stock price crashes.

Demek & Kaplan (2023) study the impact of cybersecurity breach communication from the CEO and companies cybersecurity risk management strength. The studies results show that cybersecurity risk management initiatives are positively perceived by the investors and that CEOs' statements are important in building long term trust of the management, and investors' actions. The study also finds that when companies disclose the initiatives, investors expect better protection of the firm, and that markets' reaction to subsequent events is stronger. Even in this case, the CEOs statement is important to maintain the trust of the investors and overall reputations. From an investor perspective, manager's communication is necessary, but should be carefully decided, in terms of timing and extent.

Multiple academic research papers provide various ways to quantify cybersecurity risk. One of those by Zadeh et al. (2023) developed a classification framework by evaluating severity of the breach using S&P 500 data. They introduce the Breach Level Index (BLI) that scores incidents by amount of records exposed, data sensitivity, breach source and malicious use of data, this way combining content analysis and likelihood impact matrix. The highest impact score is associated with hacking or malware, and lowest score was attributed to unintended disclosures. All this shows that breach characteristics shape the way risk is assessed and can impact the volume of financial consequences. Market reactions are better explained when the type of the cyber incident is considered together with the severity of the incident.

Tan et al. (2025) explore ESG regulation connection to cybersecurity governance. They employ machine learning analysis on Chinese Firms, showing evidence on how cybersecurity governance increases market value by building trust with investors, and strengthening supply chain connections. The stock market reacts negatively to breaches, but also reacts in a positive way to companies that perform governance changes that focus on preventing cyber incidents. Government regulation on disclosing these events provide information to investors and strengthen the reactions.

As seen in studies by Tosun (2021), Day & Booker (2024) and Huygen & Beulen (2025), there is strong evidence on how cyber incidents cause a reaction in the markets. They show strong evidence in different markets and time periods of how cybersecurity incidents are followed by immediate negative reactions in the secondary markets and also shape long term opinions on the companies reputation, leading to governance adjustments. These studies

provide a base to the first hypothesis of the thesis: Do cybersecurity incidents lead to significant abnormal returns for affected companies after a cyber incident? (Day & Booker, 2024; Huygen & Beulen, 2025; Tosun, 2021) It is important to examine this hypothesis in the event sample that was selected for this thesis.

Covered event studies show the short term drop in stock prices, but do not usually cover subsequent events, or explore what the differences are between industries. Research that covers regulation and disclosure laws show that it can increase transparency, but by providing information to investors also increases the reactions, leading to stronger negative reactions in cases of breaches. Studies on ESG and communication show that trust in companies and governance quality are both important factors in markets' response to cybersecurity incidents. To sum up, literature shows how cybersecurity risk is perceived and can change how companies are evaluated.

1.3 Cybersecurity Risk and Cost of Capital

Academic research also has been increasingly researching the relationship between cybersecurity risk and the cost of capital. This area seems to be relatively underdeveloped, especially when compared to the literature on short-term market reactions to cyber incidents (Gao et al., 2025). According to Elmawazini et al. (2023), companies' financing conditions can be influenced by cyber events by elevating their perceived risk, changing investor expectations, and shaping companies' access to debt and equity markets.

Although the cost of capital is usually analyzed by measuring Financial risk, some recent studies show that operational risks like cyber security threats, can also be incorporated into the pricing of capital, according to Florackis et al. (2022). Havakhor et al. (2021) show that financing costs can also be amplified or reduced due to disclosure practices of cyber security that contribute to the degree of information asymmetry. Although specific ways by which cyber security risk and the cost of capital are related are underdeveloped, the existing research provides a base for examining it. Introduced in Table 1, are specific angles on the research that review current evidence on three main topics: systematic risk and equity premiums, debt financing and credit risk, and the role of information asymmetry in shaping capital costs.

Recent research also covers how inventors take into consideration cybersecurity risk. Jamilov et al. (2023) cover how cyber risk is reflected in equity and option markets and indicate that investors anticipate financial consequences before the incident occurs, but also show how cyber threats are systemic and connect to suppliers, partners and possibly customers. This way cyber risks are perceived in a different way, affecting not just one company but related ones.

This confirms that investing in cybersecurity is important for businesses maintaining operations, and how companies are valued and financed in secondary markets, and that preparation for cyber incidents is important for the investors.

Agency theory provides a deeper explanation for the relationship between cybersecurity and cost of capital. As defined by Jensen & Meckling (1976), agency relationship is a contract where principals delegate decision-making authority to agents, and expect that the agent will act on their behalf. but because both of the parties are assumed to maximize utility, agents sometimes may not act in the best interests of principals. They also explain how this relationship brings in extra costs, brought by the conflict within the parties, like monitoring and bonding costs, that come from agents showing the owners that they are acting in the owners' interests, and owners spending on monitoring the agents. In a corporate context, this means that managers may have more detailed information about certain operations that can change the way that they invest or report activities. The agency problem can create inefficiencies, changing the way that risk management is planned, and that later can be seen in companies' evaluation or even financing conditions.

Recent research on cyber security governance also analyzes it from this angle. Research by Kiesow Cortez & Dekker (2022) Focuses on information asymmetry. Their findings show that the technical complexity of cybersecurity can increase information asymmetry and accountability problems. They analyze the financial sector of Benelux and identify a "common agency problem," showing that managers have to balance expectations from shareholders, employees, regulators, and customers, that are usually different. Limited communication between technical experts and stakeholders lets managers cover specific vulnerabilities, that in return leads to underdeveloped oversight and specific areas. External investors are then uninformed of these issues and are not aware of the actual risk exposure of the firm.

Havakhor et al. (2021) examine the financial implications of cybersecurity disclosure. Their study investigates how voluntary reporting of cyber security investments can influence companies' cost of capital. They use SEC comment letters as external shock to find that disclosing cybersecurity activities can lead to a reduced cost of capital. This suggests that disclosure of cyber security signals to the market, reduces information asymmetry, and allows investors to have a more accurate risk assessment. When companies provide clear and specific information and not vague statements, and when an explanation is provided by analysts to investors, the disclosure is most efficient. Voluntary disclosure reduces uncertainty, lowers the premium demanded by investors, and leads to better reputation and measurable financial results. This shows how transparency of brisk management can reduce financing costs.

Malliouris (2021) analyzes the financial consequences of severe cyber security breaches and security investments and impact on cost of capital. The findings are that credit default swaps do not consistently respond to breaches and shows that equity and debt investors perceive cyber risk differently, providing overall less conclusive evidence from debt markets. The study explains how breaches can lead to abnormal returns induced by insider trading, this way reflecting the information asymmetry. Along with the empirical results the study introduces the “Iceberg Model of Information Security Costs” that aims to measure direct and indirect costs of security investments, and provides a holistic analysis for it.

Creditors and rating agencies are also integrating cybersecurity into credit assessment frameworks. Moody’s warns that if a company has problems in their cyber detection, response or recovery capabilities after a severe cyber event, companies’ ratings can be affected by the events, increasing borrowing costs (Levy et al., 2021). S&P Global Ratings has also incorporated cybersecurity to its management and governance evaluations. They emphasize that weak cyber risk management practices can ruin creditworthiness and financial stability (*Cyber Trends and Credit Risks*, 2022). This shows how cybersecurity resilience and response to breaches is important for companies’ reputation, can impact borrowing costs and influence investors decisions.

The research on secondary debt markets does not show a clear or consistent reaction to cybersecurity events. A study by Malliouris (2021) shows how credit default swap (CDS) spreads react to bridge announcements, but does not find a consistent change there. This implies that investors in bonds and CDS do not consider cyberevents to be directly connected to default risk. Agarwal et al. (2024) show that even within limited overall market response, disclosure requirements can influence debt pricing in certain situations, but shows that investors and analysts still struggle to judge how cyber incidents affect the company's ability to repay debt. This suggests that secondary market instruments can only partially show the effects of cybersecurity risk or incidents, and how it creates a difference between actual changes in creditworthiness and perceptions of it.

Other research on loan markets indicates reactions to cybersecurity issues are more prominent within creditors than in investors. A study by He Huang and Wang (2021) shows that companies experiencing data breaches face higher loan spreads and stricter terms. This includes greater collateral requirements and tighter covenants, both affecting the company. Sheneman (2025) provides similar evidence in forecasting assessments. The study finds that companies that are perceived to have higher cyber risk pay higher interest and are more likely to face collateral requirements, tighter covenants, and “insurance sweep” clauses, that require

any cyber insurance payouts to go directly to debt repayment. Choi et al. (2025) show that if a company has a higher cybersecurity risk, lenders in syndicated loans charge higher spreads.

For commercial banks, stricter monitoring and more intensive covenants are needed. Jin et al. (2023) show how weak cybersecurity governance is related to closer inspection from banks. This shows that lenders increase loan loss provisions and oversight if there is a higher vulnerability to cyber incidents in the company. To summarize, these studies all show that creditors take cyber security risk into account when deciding the price and the conditions of lending. Companies with strong cyber security governance and transparent practices are able to get less restrictive loans. For companies with weak cybersecurity practices or low resilience, costs can be higher and terms might be stricter.

Second hypothesis is formed upon the research showing that the characteristics of cyber incidents can call different market reactions: He Huang & Wang (2021) find that certain types of incidents are causing more defined negative reactions in terms of bank loan terms, Zadeh et al. (2023) Focus on developing an index for scoring cyber incidents characteristics and also find that seriousness of the incident yield different financial outcomes, and Huygen and Beulen (2025) also find that market reactions vary, according to the category of the breach type. Therefore the second hypothesis is as follows: Are market reactions to cyber incidents systematically different based on incident characteristics? (He Huang & Wang, 2021; Huygen & Beulen, 2025; Zadeh et al., 2023). This hypothesis aims to explain the differences between market reactions, providing insight on how investors assess the cyber event.

To sum up, recent research in this area shows that cybersecurity risk now affects how companies raise capital and how the cost for it is shaped. The theory also covers how because of agency problems create information asymmetry between companies management and investors. Other empirical research analyzes how disclosure and governance practices might help produce uncertainty and can lower the premium that investors demand. Other findings from equity and debt markets show mixed results: secondary debt instruments like CDS spreads show limited reactions to breaches, and direct lending shows more direct adjustments through higher spreads, stricter covenants, and increased monitoring. From the perspective of rating agencies, cyber risk has also been incorporated into assessments of the companies. The insights from this subsection of the thesis show that strong cybersecurity governance and transparency mitigate operational and reputational risks, can support more favorable finance and conditions, but weak practices can raise the cost of equity or debt.

1.4 Strategic Investment Responses to Cyber Threats and Risk Management Frameworks

Cybersecurity investment is a very important strategic financial decision. Investments into cybersecurity can affect companies value, shape how capital is allocated, and it can have long-term effects for the company, forming reputation and competitiveness. As cyber threats are increasing with digitalization, investment into cybersecurity becomes essential, it can help to reduce risks and prevent business disruptions, maintain operationality. Because breaches can be financially costly, damage reputation and have long term financial impact for the company, and create ripple effects across supply chain and the customer, it is important for companies to have proactive cybersecurity investment (Fedele & Roner, 2022). This can be seen in practice by looking at actions of boards of directors and chief financial officers. Effective management of cyber threats falls under one of the responsibilities of the board, and is tied to fiduciary duties and the protection of shareholder value (Caluwe et al., 2024; Cybersecurity and Financial Reporting Risk: PwC, 2025). Study by Shaikh & Siponen (2023) finds that breaches that are costly receive more management attention and because of that companies conduct more formal security risk assessments. This increases the likelihood that the company will conduct formal security risk assessment as a part of the companies' enterprise risk management process.

Mizrak (2023) further adds to this research topic and shows that integrating cybersecurity into strategic management when aligned with business objectives, can strengthen resilience, and competitiveness of the company within the industry. The study explains that for cyber security to become a driver of stakeholder trust and sustained business growth, leadership needs to be committed, and the integration of this needs to be supported by the organization. These findings show how cybersecurity spending, including protective measures, creates long term value for the company.

Fedele and Ronner (2022) cover company cybersecurity Investments, by splitting the literature into four different streams. The first stream covers single firm models, where cyber security spending is evaluated in isolation, weighing expected losses against investment costs, that often lead to underinvestment. The second stream covers non-competing firms that are connected via shared networks, meaning one companies' weakness can expose others, focusing on interdependent security. The third stream covers companies that are competing, and see cyber security as an advantage. This stream invests defensively to protect their market share.The fourth stream covers companies that are competitors and also interconnected, like banks on the SWIFT network. Cyber risk for these companies is systemic and strategic. The

study indicates that different perspectives on cyber security investment decisions depend on the company and other environmental factors, like interdependence, competition, spillovers and others. If companies overestimate positive spillovers, they might invest too little. Over over investing might happen in highly competitive markets, when companies have to invest to sustain the advantage over others. Spending more or less than the optimal amount means inefficient Capital allocation and in response can create other risks for investors. In this situation regulation is important to create incentives and a balance for the industries, creating a baseline for companies investments. As explained by literature, cyber security spending is interconnected with risk reduction, regulatory compliance, research and development, and overall business operations.

Cyber security investment has multiple reasons but in literature several key topics stand out. According to Nong et al. (2025), One key reason is research and development (R&D), that is often stimulated by regulatory requirements. Nong et al. (2022) state that “implementation of the cybersecurity law significantly promotes corporate R&D investment,” and emphasize the connection between legal frameworks and innovation. One other key reason for cybersecurity investment is to prevent or reduce damage, and manage threats. Because cyber crime is expected to cause trillions of dollars and losses by 2030, companies are investing in cyber security systems to reduce risks, protect operations and continuity of the business, that is crucial in certain industries (“Cybersecurity Market Report 2025-2030 | Surge in Cybersecurity Expenditure with $1 Trillion Investment Projected by 2028,” 2025).

Some research provides evidence that financial markets already in corporate cybersecurity risk into expected returns. A research by Florackis et al. (2023) describes a way to measure cyber exposure for the company by using text analysis of corporate disclosures. They find that their measurements predict the likelihood of future incidents and expected stock returns.This shows that investors are expecting higher returns from companies with greater risk exposure and uncertainty. This shows that the investors believe that cyber risk is a systematic risk and cannot be purely random.

Companies do not rely on market reactions only when deciding how much to spend on cybersecurity. Existing literature covers how managers set the budgets based on risk assessments, regulations and past incidents, using enterprise risk management frameworks as benchmarks. This is also important because it helps managers to coordinate cybersecurity priorities across the front departments, providing more technical knowledge for the decision making. Lee (2021) create a framework for companies to justify the cyberinvestment: It is noted that the company needs to assess External threats, cyber infrastructure layer, focusing on

internal systems, employees and other, and also evaluate Risk by identifying vulnerabilities and potential impacts. Lastly the study notes that once these assessments are made, specific cyber security investment decisions can be made. This structure helps companies justify the spending by assessing the overall landscape. Study by Melaku (2023) also provides a specific framework for cyber risk management, pushing for a defined cybersecurity risk team, assigning responsibilities to specific employees or a mechanism, training employees, and maintaining an incident management plan. The framework proposed by the study is supposed to serve for strategic, tactical and operational levels.

The research is also aiming to quantify cyber risks so that the decisions in corporate finance can be backed with more confidence. Benton & Radziwill (2017) explores cybersecurity costs and the NIST cybersecurity framework. The study finds that cybersecurity costs shift between prevention, testing, and failures, and the framework provided gives the company a way to see if enough is invested into prevention or other categories. Such frameworks allow managers to see cybersecurity as a measurable cost category. Ganin et al. (2020) creates a decision analysis based approach model, also quantifying threat and vulnerability, that aims to provide structure to risk assessment and management. Quantifying cybersecurity risk or assessing it in a structured way helps managers make more informed decisions, based on a framework that reacts to changes in risk.

How these frameworks are used in practice and maintained over time has also been covered by literature. Ampel et al. (2024) develop a framework that improves how different cyber security incident types are identified and classified, then links exploits to real vulnerabilities, helping analysts detect and respond to new threats faster. Study by Melaku (2023) also describes that for frameworks to remain effective, they need to be overlooked by the board and should be evaluated continuously. The companies can improve cybersecurity decisions by using these structured Frameworks because they link first management Capital costs and overall financial performance. Companies can manage cybersecurity more effectively, compare different outcomes, and lower the risks that are closely watched by the markets.

Cyber insurance is also important when evaluating how a company manages risks. Joshi et al. (2025) compare cyber security spending and insurance by using two decision models. They find that higher investment in protection reduces expected losses and insurance costs, and insurance pricing reflects how decision makers and markets assess companies cyber risk that is left, not covered by insurance.

It is important to note that insurance does not replace direct investment. Study by Li & Liao (2025) Explains how insurance and investment are supposed to be managed together.

Some companies might over rely on insurance, ditching spending on preventative systems. Attackers might respond to this by increasing attack efforts. Because of this, investors often consider insurance useful only when it is paired with strong frameworks such as NIST or ISO[1]. Companies that combine strong controls with insurance show better governance and risk management. That can lead to more favorable financing conditions, whereas the companies that rely on insurance coverage still can be considered higher risk.

Literature covers investment into cybersecurity risk management from various angles. A study by Lee (2021) shows how cyber incidents cause various kinds of financial costs, and companies respond to that by constantly reassessing cybersecurity risk and have to adjust investments accordingly. Ganin et al. (2020) explain how cyber threats influence managers' decisions on how to allocate resources including cybersecurity investments. The studies show that companies have to assess the cyber risks that lead to how investment choices are made, leading to a question if companies also change or reassess their investment after a cyber event. Basically, companies anticipate cyber risks and prepare for them, but there is limited evidence on how companies revise the investment. This leads to the fourth hypothesis: Do cybersecurity incidents affect companies' future investment decisions? (Ganin et al., 2020; Lee, 2021)

Overall, the literature shows that companies' risk management frameworks allow companies to integrate cybersecurity into wide financial and strategic planning. Frameworks are important for both managers and investors. Managers can rely on the frameworks to tie technical controls to specific threat categories and exposure, allowing them to decide on cybersecurity spending. For investors and lenders, companies' stability and resilience is important. These frameworks connect governance, risk tolerance, and security practices that provide that information to them. Because frameworks are often tied to regulation and governance, they lead to the role of regulation, governance, and ESG in shaping cybersecurity investment that are discussed next.

1.5 Regulatory and Governance Influences on Cybersecurity Investment

Cybersecurity governance and legal frameworks are now fundamental elements of corporate strategy, influencing both resource allocation and risk management practices. Gao et

[1] The NIST Cybersecurity Framework and the ISO/IEC 27000 series are widely used standards for managing cybersecurity risk. NIST provides a structured risk management approach covering prevention, detection, response, and recovery, while ISO/IEC 27000 focuses on information security governance, controls, and continuous improvement. Both frameworks are commonly referenced in corporate governance and disclosure practices (Frameworks | NIST, n.d.; ISO/IEC 27001:2022 - Information Security Management Systems, n.d.)

al. (2025) note that “well-designed cybersecurity regulations can effectively mitigate data-breach risks”, providing oversight and defining accountability, which positions cybersecurity as a key aspect of enterprise risk management. At the same time, the introduction of new regulations and stricter requirements has made cybersecurity a more resource-intensive and closely regulated area of corporate management. In the following sections several key cybersecurity and legal frameworks from different jurisdictions will be introduced, that have been summarized in Table 1.

The Network and Information Systems Directive (NIS2 Directive), implemented in December 2022, represents a major overhaul of the European Union’s cybersecurity framework, replacing the original NIS Directive of 2016 (NIS2 Directive: Securing Network and Information Systems | Shaping Europe’s Digital Future, n.d.). NIS2 was updated later - it introduces stricter security requirements, expands coverage to more sectors, addresses supply chain vulnerabilities, and strengthens oversight and reporting (Vandezande, 2024). Study by Joswig and Kurz (2025) explains how the NIS2 Directive imposes risk management measures and reporting obligations requiring firms (specially SMEs) to allocate sufficient resources for compliance. NIS2 demonstrates how cybersecurity frameworks can shape financial strategy and investment decisions by connecting regulatory compliance and corporate risk management.

The General Data Protection Regulation (GDPR) was put into effect in May 2018. It sets strict rules for the collection, processing, and storage of personal data in the European Union. Beyond protecting privacy, GDPR has significant financial implications for firms, because of the non-compliance fines, which can reach up to 20 million euros or 4% of global annual turnover (Wolford, n.d.). As discussed by Boggini (2024), Article 32 describes how companies are required to implement appropriate technical and organizational measures, including encryption, multi-factor authentication, offsite backups, regular testing and others, to ensure confidentiality of personal data. Some of these obligations put pressure on companies to invest in important data governance and cyber security measures, and can influence capital allocation or budget decisions. Companies that demonstrate strong compliance with the regulations such as GDPR, aside from risk management practices, sometimes can be perceived as lower risk and signal to the market about strong data governance. Data protection is important to incorporate into risk management, because absence of it would send a negative signal to the markets.

The Securities and Exchange Commission (SEC) is constantly strengthening the requirements for the disclosure of cybersecurity risks and incidents for publicly listed firms. SEC requirements include timely and transparent reporting of material cyber threats, breaches, and mitigation measures, which lets investors to better assess firms’ risk exposure (SEC.Gov | SEC

Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies, 2023). Companies in order to meet these applications, should already have a strong cyber security infrastructure in place, including continuous monitoring, and strong governance structures. For a company to have a decent place certain strategic and financing decisions on cybersecurity monitoring already have to be present, or developed. SEC regulation aims to improve connection between cyber resilience, financial strategy, and long-term corporate performance, which is possible because of integrating cybersecurity coverage into mandatory reporting frameworks.

The Digital Operational Resilience Act (DORA), adopted in January 2023 and fully enforceable since January 2025 is one of the most significant recent regulatory initiatives in cybersecurity and operational risk management. Dora introduces a framework for managing information and Communications technology (ICT), and cyber security risks and the financial sector (Digital Operational Resilience Act (DORA) - EIOPA, n.d.). DORA puts a lot of focus on financial institutions and critical ICT service providers by requiring uniform standards for risk management, incident reporting, resilience testing, and third-party oversight (Karakasilioti, 2024). Research by Clausmeier (2022) shows how DORA leaves space for companies to follow the rules without overdoing them, and adjust how strict they are based on how big the company is and how much risk they face. The act also creates a single system to supervise key ICT providers. The set of rules oversees these providers in finance and can also be used by other industries that outsource critical technology. DORA also strengthens governance and transparency and that is important in reinforcing market trust in financial resilience. As noted by Grima & Marano (2021), “DORA is perceived as an asset ensuring prudential risk resilience in the operation of insurance, maintaining sensitivity to the needs of stakeholders and objectivity to market participants”. It may improve resilience and investor trust, but can be expensive to implement for certain companies. DORA helps companies improve trustworthiness, but it is still unclear on how these rules benefit the company.

Cyber security and data governance has also been integrated increasingly into ESG reporting frameworks. Large companies were firstly required to disclose non-financial risk by The European Union’s Non-Financial Reporting Directive (NFRD). This was followed by the Corporate Sustainability Reporting Directive (CSRD), which expanded the scope and depth of mandatory disclosures (Corporate Sustainability Reporting - European Commission, n.d.). Some recent studies highlight how these frameworks link digital resilience and data protection to ESG ratings and creating reputational and financial incentives for firms to demonstrate strong cyber governance (Balboni & Francis, 2025; Bruno et al., 2025). Another study, Liu & Shao

(2025), explains how the board of directors that take ESG seriously are usually better at managing cyber and fintech risks. Paying attention to ESG pushes managers to watch technology risks more closely and respond appropriately. ESG frameworks motivate companies to view cybersecurity as part of the ESG profile. To tie ESG back to corporate finance, cyber practices that were integrated for ESG can also reduce information asymmetry, support higher ESG ratings and by doing that, possibly reduce risk premiums demanded by creditors or investors.

A study by Fischer-Hübner et al. (2021) analyzes cybersecurity problems and challenges in critical European sectors: open banking, supply chains, privacy-preserving identity management, security incident reporting, maritime transport, medical data exchange, and smart cities. The study is based on 63 stakeholder interviews. Key findings of the study find common challenges and common requirements within the industries. Stakeholders are expecting resilience systems and infrastructures. The paper describes cybersecurity risk as a systemic risk that cannot not be managed in isolation and for this reason requires specific regulation and governance.

According to the World Economic Forum Global Cybersecurity Outlook report (2025), “Regulations are increasingly seen as an important factor for improving baseline cybersecurity posture and building trust” (*Global Cybersecurity Outlook 2025 | World Economic Forum*, 2025). Empirical research by Gao et al. (2025) supports this perspective. Their study shows that cybersecurity regulations improve companies’ cybersecurity, especially in non-state-owned Enterprises and industries that are high-tech. Regulations serve as a strengthening factor for company level resilience and risk management.

Mandatory disclosure requirements and governance obligations force management to integrate cybersecurity risk management into decision making, including financial decisions, and provide stakeholders with specific information of potential threats and companies preparation state. Studies show that compliance with the regulation strengthens investor confidence (Joswig & Kurz, 2025). According to a paper by Kiesow Cortez & Dekker (2022), regulations encourage risk mitigation and resilience and also help management and stakeholder expectations to align. Regulatory pressures push for strategic cybersecurity investment and increase the importance of legal compliance by introducing fines and other tools. NIS2, GDPR and SEC disclosure rules and ESG and DORA reporting frameworks, can influence operational security, which is especially important in critical sectors. They shape financing conditions, reputational risk, and other variables that are important for a company's value.

The regulations encourage clear and informative communication with the stakeholders. As seen, some research covers how important communication after the incident is in shaping how cyber incidents and companies' resilience to risk is perceived by the markets. Demek & Kaplan (2023) find that statement from the CEO after the breach is important and builds long term trust in the company, and how necessary the manager's communication to the public is, and study by Day & Booker (2024) highlights the need for clear communication to mitigate the market reactions. This leads to the third hypothesis of this thesis, which is: Do companies with higher quality communication post-incident experience milder negative market reactions? (Day & Booker, 2024; Demek & Kaplan, 2023).

Although in recent decades research has advanced linking cybersecurity to corporate finance, some gaps still remain. Existing work is concentrated in specific contexts that are mostly focused on the United States, Western Europe markets. This leaves smaller and mid sized firms and specific regions comparatively underexplored. Most prior studies also rely on databases such as CRSP or Thomson Reuters Datastream that are global in scope, but their coverage is uneven across regions. CRSP is built around NYSE, NASDAQ and AMEX listings that include additional data, but is mostly a U.S. equity database. Thomson Reuters Datastream has worldwide coverage, but depth and details of data are different across countries, with strongest coverage still being North America, Western Europe and some Asia and Pacific markets. Evidence from Northern or Central Europe remains underresearched, even though exposure to cyber incidents is increasing and regions are highly digitalized.

Research consistently shows that cybersecurity breaches affect firm value, but investor risk perception and other financing decisions, company responses, communication, remediation and strategic changes are not examined in depth across markets. The connection between cybersecurity regulations and firm financing conditions is still developing in the literature. Evidence of how cybersecurity investment and risk management practices influence financing costs is also fragmented and mostly based on large corporations in the U.S., therefore under different regulations. For smaller sized companies as well as companies based in less studied markets, it is less clear on how cyber incidents influence investment policies or risk management decisions. This gap points to the relevance of a region specific and mixed method approach to study this relationship.

2. METHODOLOGY

This section introduces and describes the research methodology used in the thesis. It outlines the structure of the methodological approach including the research design, data sources and analysis components. The theoretical foundations of the research are presented, with definitions, terms and concepts. This part also explains the reasoning for the chosen method, by reviewing existing literature and previous researchers' opinions on methods and limitations.

2.1 Aim and research questions and method selection

The aim of this thesis is to examine how cybersecurity incidents affect firm value and what these reactions imply for investment decisions and cost of capital and the Nordic, Baltic, and Polish markets. It is done by identifying whether the cyber events trigger measurable market responses and how differences in incident severity and firm communication shape those outcomes. To meet this aim, the following hypotheses are raised:

H1: Do cybersecurity incidents lead to significant abnormal returns for affected companies after a cyber incident?

H2: Are market reactions to cyber incidents systematically different based on incident characteristics?

H3: Do companies with higher quality communication post-incident experience milder negative market reactions?

H4: Do cybersecurity incidents affect companies’ future investment decisions?

The connection between cybersecurity risks and their effect on corporate investment decisions has been explored by several researchers. Although this research area remains concentrated in specific regions and contexts, reviewing these studies helps to identify a methodological approach that is most suitable for analyzing financial effects of cyber events in the Nordic Baltic and Polish markets. This region is selected for the analysis because of the lack of evidence or research on this region on cyberincident effect on markets, especially compared to the United States or other countries in Europe that have similar levels of digitalization or cyber crime.

The event study methodology is commonly used to measure how financial markets react when new information becomes public. The approach focuses on abnormal returns around a clearly defined event date and compares them to returns, predicted from a prior estimation period, that is based on the Efficient Market Hypothesis which states that security prices reflect all available information and adjust once new information is released (MacKinlay, 1997). This structure allows researchers to estimate the economic impact of an event by examining how

actual returns differ from expected returns in a short event window. As shown by Konchitchki & O'Leary (2011), event studies are widely applied in finance, accounting and information systems to assess market reactions to mergers, regulatory changes, management announcements, cybersecurity incidents and similar events.

As summarized in Table 2, the main studies that analyzed financial effects of cyber incidents for the most part rely on the event study methodology with similar structure; estimation windows ranging from around 200 to 255 trading days, and short event windows from one to a few days after the announcement. Huygen & Beulen (2025) quantify the short and long term valuation effects of cyberattacks by estimating expected returns over a 200 day estimation window and short event windows. Tosun (2021) uses a similar even study framework with factor model regressions and tests on trading volume and liquidity. The study shows that security breaches lead to statistically significant negative excess returns and indicate disruptions in normal trading activity. Cao et al. (2024) use a panel difference-in-differences design. Their approach exploits staggered law adoption and not exact incident dates, analyzing long term structural effects on firm risk. Malliouris (2021) applies abnormal returns analysis to cybersecurity certifications and estimated expected returns using a [-255, -4] estimation window and event windows ranging up to [-3, +2] for evaluating market reactions to firms' disclosures of new security compliance credentials. Event studies provide precise identification around cyber incident dates, require clean event windows and trading history.

Table 2

Overview of empirical event study designs in reviewed studies

Author	Purpose	Estimation window (days)	Event window (days)
Huygen & Beulen (2025)	Stock price reaction to cyber incidents	-205 to -6	[-3, +0], [-3, +1], [-3, +5]
Cao et al. (2024)	Market impact of data breach disclosure	-252 to -30	[-3, +3], [-1, +1], [-2, +2]
Tosun (2021)	Market reaction to hacking events	-3, -4, and -5 months to -30	[-1, +1], [-1, +2], [-1, +3], [-2, +2]
Malliouris (2021)	Certification events and stock reaction	-255 to -4	Ranging from -3 to +2

Source: Compiled by the author.

Table 2 also displays how the estimation window periods and event window periods are similar even when the purpose of the studies are different. Based on the summary of event studies in Table 2, for this study the selected estimation window is -235 to -5 trading days before the event announcement date. The event windows are also selected: [-1, +1], [-2, +2], [-3, +3] trading days. The event windows and estimation windows that align with previous research are chosen based on existing literature.

2.2 Qualitative and quantitative analysis design

The quantitative analysis is performed using a standard event study structure introduced earlier, focusing on estimating normal returns, identifying abnormal returns around the event date, and aggregating effects over predefined event windows. The event date is defined as the first verified public announcement of the cybersecurity incident. A relative time variable is constructed for each trading day according to the event date.

The estimation window is set from -235 to -5 trading days prior to the event. This range provides a consistent number of observations across all firms and excludes the period close to the event date to avoid including rumors and information leakage. Three symmetric event windows are used in the study to measure short term market response: [-1, +1], [-2, +2], [-3, +3] trading days. The range is in sync with previous work, overviewed in Table 2.

Daily expected returns are estimated using the market model, which compares each day's stock return to the return that would normally be expected in the absence of the event.

For each firm (i), the relationship between firm returns and market returns over the estimation period(t) is specified as:

$$R_{i,t} = \alpha_i + \beta_i R_{m,t} + \varepsilon_{i,t} \qquad (1)$$

Here, $R_{i,t}$ is daily return of company i,$R_{m,t}$ is corresponding market index, α,β are parameters estimated by ordinary least squares (OLS) using data from the estimation window, $\varepsilon_{i,t}$ is the error term.

Abnormal returns during the event windows are calculated following this formula:

$$AR_{i,t} = R_{i,t} - \left(\widehat{\alpha_i} + \hat{\beta} iRm, t\right) \qquad (2)$$

Here, $AR_{i,t}$ is the abnormal return of company i on the day t. $\widehat{\alpha_i}$and $\hat{\beta}$ are the estimated market model parameters.

Cumulative abnormal returns (CARs) for each event window are calculated as the sum of abnormal returns across days t in the selected window:

$$CAR_i(\tau_1, \tau_2) = \sum_{t=\tau_1}^{\tau_2} AR_{i,t} \quad (3)$$

$CAR_i(\tau_1, \tau_2)$ is the total impact of the incident on the company between days T and T. The market model parameters α,β are estimated for each event case using OLS over the estimation window. Here α is to show how much of the companies return is not related or caused by overall market movements, and β is the coefficient of how strongly the stock moves with the market index. These parameters are there to calculate expected returns during the event window, and see if the market model fits the data well. Summary statistics of these parameters in the research are needed to assess how reliable the model is across the companies.

These measures form the base for assessing if cyber security incidents generate statistically meaningful deviations from expected performance. The procedure is selected following established event study methodologies and is aligned with the structure defined in MacKinlay (1997), and has been used in cyber security related finance research.

Then abnormal returns and cumulative abnormal returns statistical significance is assessed using one sample t-tests that evaluate if the mean abnormal performance differs from zero. The tests are applied to daily ARs and to CARs for each event window.

A cross-sectional analysis then is conducted to check for variation in CARs and if it can be linked to characteristics of the event, an analysis that is used when market response is weak (MacKinlay, 1997). Events are grouped into categories by industry, actor type and technical attack subtype. The events are grouped to see heterogeneity in outcomes across the sample.

Alongside the event study framework, this thesis incorporates a qualitative part, to examine how companies communicate and respond to cybersecurity incidents. The qualitative analysis will follow a structured document review approach. It will be based on publicly available sources (such as press releases, regulatory disclosures, investor announcements, annual reports and communications), that were issued day of and after the incident. These documents are collected for each selected company in the event sample to assess both immediate statements or announcements, and communication issued later.

The structure used to analyze these materials is based on established research on cybersecurity crisis communication, incident response and organisation risk management. Previous literature shows that the way companies communicate cybersecurity incidents can shape stakeholder perceptions and reputation of the company, and that different types of incidents require different communication strategies (Confente et al., 2019; Knight & Nurse, 2020; Senarak, 2025). Other studies emphasize the importance of the governance within the company, resource allocation and defensive investment (Gao & Calderon, 2025; Moussa & Zine-Dine, 2025; Pigola et al., 2024).

Following the literature, five categories were defined, provided in Table 3. In case of a company not addressing a category in its public announcements, it is classified as “not covered”. In this way, lack of disclosure becomes information about transparency of the company. These categories enable a structured comparison across firms and support the interpretation of the results from quantitative analysis.

Table 3

Qualitative categories and supporting literature

Category	Relevant source
Timing	Senarak (2025), Knight & Nurse (2020)
Remediation	Senarak (2025), Pigola et al. (2024)
Investment in cybersecurity	Pigola et al. (2024), Moussa & Zine-Dine (2025)
Governance within company	Gao & Calderon (2025)
Communication strategy	Confente et al. (2019), Knight & Nurse (2020), Senarak (2025)

Source: Compiled by the author.

Timing category is based on research showing that continuous updates are necessary for transparency during cyber incidents. Remediation captures if the firms explain if and how the incident was contained, including recovery communication. Investment in cybersecurity seeks out companies statements on investment in cybersecurity capabilities, future spending or resource allocation. Governance within the company focuses on how cyber risk is tied to corporate governance, boards expertise and disclosure quality. Lastly, communication strategy is capturing how firms frame and explain the incident to stakeholders, including the structure of the statements.

This approach allows comparison across incidents and allows identifying recurring patterns. The categories selected for analysis follow existing research and are selected because of their importance on cybersecurity risk management in the corporate environment. The qualitative findings complement the event study results by providing context to investor behavior, highlight disclosure practices and most importantly companies risk management and investment decisions.

The model of qualitative analysis follows the following structure: the first step is collecting all available corporate communications for the selected firms from publicly accessible reliable sources. Second, each document is reviewed and evaluated according to the predetermined categories described above. Third, the company's information is synthesized,

checking for each category and summarizing the communication where needed. Lastly patterns across firms are compared and interpreted together with quantitative event study results. Systematic assessment of communication and other statements provides insights for differences in market reactions, investment decisions and governance responses across firms.

To examine if qualitative differences in companies responses are associated with differences in market outcomes, CARs were compared across the categories. Mean CARs are calculated for firms grouped by the categories selected above. This approach allows us to assess if firms that respond differently to cyber incidents experience systematically different short term market reactions.

The empirical findings should be interpreted in context of following methodological limitations. The limited number of events reduces the ability to detect statistically significant effects and increases the sensitivity to company specific outcomes. This is relevant especially for cross-sectional analysis, where some categories contain only a few observations. Cybersecurity incidents vary in nature, scope and disclosure quality, which introduces differences that cannot be fully controlled for in this case. Also, qualitative assessment is constrained by the availability and timing of corporate disclosures, which may understate governance or investment responses that are not publicly communicated. The use of short term event windows captures immediate reaction but does not reflect longer term adjustments.

2.3 Data sources and variables

The cyber incidents data is constructed using the University of Maryland CISSM Cyber events database (Gallagher & Harry, 2023). It is an open repository recording cyber incidents worldwide. It provides structured records from 2014, updated monthly, and is used in multiple cybersecurity research papers, including Huygen & Beulen (2025) and Caluwe et al. (2024). The database is valued for consistent reporting event dates, companies that experienced the incidents (the victims) and sources for the incident announcements.

From the full set of 501 events recorded for the Nordic countries, Baltic Countries and Poland, only incidents that occurred to listed companies were retained. Initial filtering removed events targeting municipalities, government agencies, airports, government owned healthcare institutions, educational institutions and other public sector entities, and companies that are not listed. This filtering left a list of 49 incidents. Incidents occurring before 2015 were excluded because the event study estimation window requires 250 days before the event data, and financial data available only provide information of ten most recent years of historical prices at the time of extraction. Some events were removed due to the selected estimation window unable to meet the minimum amount of trading days.

All seven Spotify related events were excluded: although Spotify is headquartered in Sweden, it has been listed on New York Stock Exchange since April 2018 (*Contact - Spotify*, n.d.; *Spotify Lists on NYSE as SPOT - Spotify*, 2018). This means including the cyber incidents of Spotify would include the analysis of US markets; 5 events that happened prior the company's listing date have been excluded as well.

Duplicate incident entries with identical descriptions were treated as database (coding) errors and were treated as one. After cleaning the data, the final dataset includes 28 cyber events between 2017 and 2025 for Denmark, Finland, Latvia, Lithuania, Norway, Poland and Sweden. It represents a region that is highly digital, follows governance and cybersecurity and disclosure regulations from the EU/EEA region and are comparatively understudied, compared to the United States markets.

Data for the quantitative analysis has been collected from multiple sources, two main components are market index data for each event's listed market, and historical data of the companies closing prices on selected periods for estimation and event windows. Data for the market index corresponding to each company's country is used as a benchmark for the return series in the market model. Index data are obtained directly from Nasdaq Global Index watch for firms listed in Nordic and Baltic countries, for Copenhagen stock exchange - OMXCPI, Helsinki - OMXHGI, OMX Stockholm - OMXSGI, Riga OMXRGI, Vilnius OMXVGI (Nasdaq Global Index Watch, n.d.). Warsaw (WIG) was accessed through the official Warsaw Stock Exchange website (GPW Main Market - Main Market, n.d.). These benchmarks reflect the performance of the markets in which companies are listed and help estimate normal returns. Daily index levels were used for the full estimation windows and event windows, then converted into percentage returns. The use of domestic market indexes aligns with standard event study methodology.

For the events from companies CD Projekt Red, Sandvik, Maerks, Ericsson, Norsk Hydro, AKVA, Ignitis Group, Polska Group Energetyczna, PKP Cargo, Tele2, Telia, REC Silicon, Tomra, Valmet, Nokia, Assa Abloy, Asseco Poland S.A., Eezy Plc, Panostaja Oyj, Taaleri Plc, Pandora, DSV, the historical data was sourced from Financial times (Akva Group ASA, AKVA:OSL Historical Prices - FT.Com, n.d.; AP Moeller - Maersk A/S, MAERSK B:CPH Historical Prices - FT.Com, n.d.; Assa Abloy AB, ASSA B:STO Summary - FT.Com, n.d.; Asseco Poland SA, ACP:WSE Historical Prices - FT.Com, n.d.; CD Projekt SA, CDR:WSE Historical Prices - FT.Com, n.d.; DSV A/S, DSV:CPH Historical Prices - FT.Com, n.d.; Eezy Oyj, EEZY:HEX Historical Prices - FT.Com, n.d.; Ignitis Grupe AB, IGN1L:VLX Historical Prices - FT.Com, n.d.; NOKIA, NOK1V:HEX Historical Prices - FT.Com, n.d.; Norsk Hydro ASA, NHY:OSL Historical Prices - FT.Com, n.d.; Pandora A/S, PNDORA:CPH Historical Prices -

FT.Com, n.d.; Panostaja Oyj, PNA1V:HEX Historical Prices - FT.Com, n.d.; PGE Polska Grupa Energetyczna SA, PGE:WSE Historical Prices - FT.Com, n.d.-a; PKP Cargo SA w Restrukturyzacji, PKP:WSE Historical Prices - FT.Com, n.d.; REC Silicon ASA, RECSI:OSL Summary - FT.Com, n.d.; Sandvik AB, SAND:STO Historical Prices - FT.Com, n.d.; Taaleri Oyj, TAALA:HEX Historical Prices - FT.Com, n.d.; Tele2 AB, TEL2 B:STO Historical Prices - FT.Com, n.d.; Telefonaktiebolaget LM Ericsson, ERIC B:STO Historical Prices - FT.Com, n.d.; Telia Company AB, TELIA:STO Historical Prices - FT.Com, n.d.; Tomra Systems ASA, TOM:OSL Historical Prices - FT.Com, n.d.; Valmet Oyj, VALMT:HEX Historical Prices - FT.Com, n.d.). For Delfin Group and Hansamatrix, the data was sourced from Nasdaq Baltic website (DelfinGroup | Trading — Nasdaq Baltic, n.d.; HansaMatrix | Trading — Nasdaq Baltic, n.d.).

Daily stock returns were calculated as percentage change in closing prices from closing prices obtained from the sources described above. Market returns were calculated in the same way using the percentage change in daily closing value of corresponding domestic benchmark index. These return series are the basis for estimating normal returns in the market model introduced earlier.

Initial data collection and cleaning were carried out in Microsoft Excel. The final dataset preparation, event study calculations and statistical analysis were carried out in Python.

The time variable is relative to the event. It is constructed by aligning all trading days around the cyber incident disclosure date. The event date is defined as the first verified public announcement of the cyber incident and is denoted as $t = 0$. Trading days before the event are expressed in negative values, and days after are positive values. With this structure each observation, an estimation window and events windows are consistent throughout the events and is appropriate for further analysis.

Abnormal returns (AR) were computed as the difference between actual returns and model predicted returns for each event window day, and CARs were obtained by summing AR values for each window. These form the main quantitative variables used in the empirical analysis.

Additional variables were constructed for qualitative to represent incident characteristics and firm responses. The qualitative categories are treated as explanatory variables that describe companies' cybersecurity response characteristics. They are later used to group firms and compare CARs across response types, allowing assessment of whether differences in communication, remediation, governance, timing and investment decisions are associated with different market reactions.

3. EMPIRICAL RESEARCH

In the following part of the thesis empirical research is conducted to evaluate how cybersecurity incidents affect firm value and what these reactions imply for risk perception and investment decisions. The data and variables selected and used are described and presented. That is done by applying the research methodology described and chosen prior. The results are analyzed and interpreted in line with the aims of the thesis.

3.1 Descriptive analysis, estimation windows and market model fit

The final dataset consists of 28 cybersecurity incidents. The distribution of events is uneven across countries: Poland accounts for the largest amount - 8 events, followed by Finland with 5 events, Sweden - 5 events, Norway with 4 events, Denmark 3 events, Lithuania with 2 and Latvia 1 event. This displays regional differences in size of markets. Incidents are recorded in a wide range of industries. Most represented within listed companies are manufacturing (6 events) and utilities (5 events), then followed by transportation and warehousing (4 events), arts, entertainment and recreation (3 events) and information (3 events). Other sectors such as finance and insurance, professional and technical services, retail trade and wholesale trade appear one or two times. The distribution illustrates that incidents occur in various industries, but production intensive sectors are more frequently appearing in the sample.

Distribution between years does not show a clear trend; it is important to note that data has been cleaned and only events that fit under certain criteria were selected. Highest number of incidents per year from the sample was 2022, with 9 events, lowest - 2018, 2019 and 2024 with one each, and 2020 with no events.

Estimation window, as has been described earlier, has been set and defined as $t = -235$ to $t = -5$ trading days prior to the cyber incident announcement. All events include sufficient trading day coverage for model estimation. Each event has data for at least 235 trading days prior to the event, ensuring that all regressions are based on the same sample length. Post event trading day availability also exceeds the minimum selected amount of trading days for selected event windows. This way the estimation windows are aligned across firms and are consistent within the data sample, and are suitable for market model estimation.

The next step after selecting the event window was to estimate the parameters obtained from the market model. The parameters α and β of the market model were estimated using OLS over the estimation window, ending prior the cybersecurity incident. Low α (0) would mean a stable return model. The β indicates stock return sensitivity to the market movements, with 0

representing no reaction to market, and 1 would mean market-sensitive stock movements. The descriptive statistics for estimated parameters are presented in Table 4 below.

Table 4

Descriptive statistics for α and β parameters

	mean	std	min	25%	50%	75%	max
alpha	0.000687	0.001928	-0.00379	-0.00058	0.00064	0.001684	0.004352
beta	0.770931	0.455932	-0.28588	0.406447	0.996412	1.083361	1.517413

Source: Calculated by the author based on data from Nasdaq Baltic Stock Exchanges Home Page (n.d.) and Markets Data - Stock Market, Bond, Equity, Commodity Prices - FT.Com (n.d.).

Table 4 shows that alpha values are concentrated around zero, with mean being 0.000687 and median 0.00064. There is not a lot of variation across the firms. This shows that firms do not display systematic abnormal returns within the estimation window. This also does not show information leaks prior to the incident. The beta values vary more, from -0.28588 to 1.517413. The mean is 0.770931 and median 0.996412. This indicates slightly left-skewed distribution. Based on the interquartile range, most firms have moderate market sensitivity and so the average stock moves less than the market. The wide spread of beta values shows different firm returns in response to the broader market. This variation in case of event study is important because the market model adjusts expected returns using each firm's individual beta estimate. These differences in market sensitivity have an effect on how abnormal returns are measured. The beta variation could also be attributed to the event sample including several industries and event types. Full table of alpha and beta values for incidents are attached in Annex 2.

To test the first hypothesis, “Do cybersecurity incidents lead to significant abnormal returns for affected companies after a cyber incident?“, abnormal returns and cumulative abnormal returns are analyzed. Here, the next steps are to assess how stock prices react around the event date. Abnormal returns (ARs) were examined for each trading day from t=-3 to t=+3. These values reflect the difference between actual returns and the estimated returns earlier calculated by using the market model. Then average is taken of the ARs for all events and for each event day, in order to see if firms in the sample experienced a common price reaction and the defined event window.

Table 5 below presents the mean ARs for each day in the [-3, +3] event window. The results show that ARs fluctuate around zero in the days prior to the event day. On t=-3 the average AR is 0.0015, on t = -2 is -.0040, and on t = -1 it is -0.0012. These values are small and

show no consistent direction. This points to no clear sign of information leakage. On event day (t=0), the AR is positive (0.0042), suggesting that on average firms did not experience an immediate negative price reaction on the day of public announcement. The following days after the event also showed mixed results, t=1 was -0.0092, t-2 was 0.0021, t=3 was -0.0029. These movements also show no trend and are relatively small movements. The ARs do not indicate a strong reaction, and point to a weak or inconsistent short term market reaction over the event window.

Table 5

Mean Abnormal Returns (AR) for event days (t)

t	AR
-3	0.0015
-2	-0.0040
-1	-0.0012
0	0.0042
1	-0.0092
2	0.0021
3	-0.0029

Source: Calculated by the author based on data from Nasdaq Baltic Stock Exchanges Home Page (n.d.) and Markets Data - Stock Market, Bond, Equity, Commodity Prices - FT.Com (n.d.).

One sample t-test was performed for each event day to test if the mean ARs differ significantly from zero. None of the ARs are statistically significant, p-values for all days were above 0.1 including the event day, where t-statistic was 0.539 and p-value was 0.596 show that the return is not statistically meaningful. Pre-event days also display no significance, supporting the no information leak. Post-event aRs are also small and statistically insignificant. In this case the results suggest that the short term abnormal returns around the event date show that none of the movements around the date are statistically significant.

Cumulative abnormal returns (CARs) were calculated for three symmetric event windows to assess the short term price reaction to the incident. Consistent with the event study methodology, CAR provides a clear measure of market reaction when daily abnormal returns are small or volatile (MacKinlay, 1997).

The CARs were calculated for each event, and each event window. Full results are attached in the Annex 1. Table 6 below provides the summary statistics for the three CAR event windows. The mean CARs are small and negative across all windows. For the [-1, +1] window, the mean CAR is -0.0047, for the [-2, +2] window is also close to zero (0.005), for the [-3, +3] window it is 0.0066. These values indicate a very slight negative movement in share prices during the event period. The standard deviations range from 0.0384 to 0.0555, showing considerable variations across events. The minimum and maximum CAR values also indicate some firms experienced more pronounced movements in either direction, but these cases do not reflect the overall sample. This cross-sectional spread is typical in event studies with heterogeneous firms and industries.

Table 6

Summary statistics for CARs across event windows

Window	mean	std	min	max
[-1, +1]	-0.0047	0.0384	-0.067	0.069
[-2, +2]	-0.005	0.048	-0.1068	0.0981
[-3, +3]	-0.0066	0.0555	-0.1081	0.1066

Source: Calculated by the author based on data from Nasdaq Baltic Stock Exchanges Home Page (n.d.) and Markets Data - Stock Market, Bond, Equity, Commodity Prices - FT.Com (n.d.).

One sample t-tests were conducted for each event window to test if the mean cars differ from zero. The results are shown in Table 7. They indicate that none of the CARs are statistically significant. All the p-values are above significance levels and t-statistics are small in absolute value (between -0.55 and -0.64). This means that the average cumulative returns cannot be distinguished from zero in any of the three windows.

The CAR t-test evaluates the combined effect of several days around the event, and does not just focus on individual abnormal returns. It provides a more stable estimate of the overall price reaction. Even when using cumulative returns, the results do not show a systematic market response. This suggests that any short-term impact of the incidents is small relative to normal return variation and is not strong enough to produce statistically meaningful deviations over the event period.

Taken together the results show no statistically meaningful short term reaction to the incident disclosures in this dataset. Although the average CARs are negative, the magnitudes

are small and not statistically significant. The results also show that variation in firm characteristics and the relatively small sample size may limit the power of the tests.

Table 7

CAR significance tests t-statistics and p-values

window	t_stat	p_value
[-1, +1]	-0.6416	0.5266
[-2, +2]	-0.5518	0.5856
[-3, +3]	-0.6278	0.5354

Source: Calculated by the author based on data from Nasdaq Baltic Stock Exchanges Home Page (n.d.) and Markets Data - Stock Market, Bond, Equity, Commodity Prices - FT.Com (n.d.).

These results indicate that the first hypothesis, which tests if cybersecurity incidents lead to significant abnormal returns after a cyber incident, is rejected. There is not enough evidence on statistical significance, which could be due to a small sample size. Mean CARs are negative, but small. One sample t-tests fail to reject the null hypothesis, for all event windows. This leads to conclusion that there is no proof of systematic reaction to the cyber incidents in the event seen in the markets, short term after the incident.

3.3 Cross-sectional analysis

This section examines if the variation in the cumulative abnormal returns across events can be linked to observable characteristics of the incidents. Average CARs do not show a significant market reaction at the aggregate level, individual events have different attributions, such as industry, attacker type, motive and others. In the following sections it is explored if these factors can explain the cross-sectional dispersion.

Table 8 displays mean CARs by industry for three event windows. The results show variation across industries. Some sectors display small positive CARs, such as Administration and Wholesale Trade. Some show consistently negative values, including Arts, Entertainment and Recreation, Professional Services and Information. Manufacturing and Utilities have values closer to zero, with limited variation. Even when split by industry, these differences are still not statistically significant, but industries with higher operational dependence on digital systems or greater exposure to reputational risk tend to show more negative CARs. Even with aggregate market response remaining weak, some of the differences highlight that market reactions may reflect perceived vulnerability or business continuity in the affected sector.

Table 8

CARs by industry for event windows

Industry/ Window	[-1, +1]	[-2, +2]	[-3, +3]
Administrative and Support and Waste Management and Remediation Services	0.0248	0.0389	0.0371
Arts, Entertainment, and Recreation	-0.0235	-0.0321	-0.0484
Finance and Insurance	0.0166	0.09	0.0708
Information	-0.0222	-0.0187	-0.0275
Manufacturing	0.0141	0.0055	0.0206
Professional, Scientific, and Technical Services	-0.067	-0.1068	-0.1081
Retail Trade	-0.0091	-0.0082	0.0005
Transportation and Warehousing	0.0137	0.0003	0.0018
Undetermined	-0.0510	-0.0336	-0.0606
Utilities	-0.0108	-0.0211	-0.0183
Wholesale Trade	0.0309	0.0254	0.0357

Source: Calculated by the author based on data from Nasdaq Baltic Stock Exchanges Home Page (n.d.) and Markets Data - Stock Market, Bond, Equity, Commodity Prices - FT.Com (n.d.).

CARs summarized by actor or attacker type are summarized in Table 9. Event types attributed to criminal actors show consistently negative CARs across all event windows. Meanwhile activist and nation-state attributed accidents display very small but positive average CARs. These patterns suggest that investors may interpret attacks differently based on the intention or type of the actor. The differences are not statistically significant as well, but the direction of the impact is consistent across windows when split by the actor types. This can possibly indicate that the attacker type may influence market reactions about the consequences of the incident.

Table 10 below represents the results of CARs grouped by event subtype. Application exploitation, data attack, denial of service, and last category for unknown (1 event). The results show clear stable differences between these classifications. Data attacks show the most negative CARs and become more negative as the window widens. Application exploitation also

shows small negative values. Denial of service events display positive CARs across all windows. This pattern could indicate that markets view confidentiality breaches and data loss as more financially damaging events than service disruption attacks that are often temporary and less costly. The unknown category shows more negative CARs but can be attributed to just small group size.

Table 9

CARs by actor type for event windows

Actor type	[-1, +1]	[-2, +2]	[-3, +3]
Criminal	-0.0164	-0.0205	-0.0217
Hacktivist	0.012	0.0115	0.0114
Nation-State	0.0032	0.0073	0.0041

Source: Calculated by the author based on data from Nasdaq Baltic Stock Exchanges Home Page (n.d.) and Markets Data - Stock Market, Bond, Equity, Commodity Prices - FT.Com (n.d.).

Table 10

CARs by country of the event for event windows

Event subtype, grouped	[-1, +1]	[-2, +2]	[-3, +3]
Application Exploitation	-0.011	-0.0178	-0.0129
Data Attack	-0.0158	-0.0143	-0.0232
Denial of Service	0.0106	0.0104	0.0101
Unknown	-0.0589	-0.0226	-0.0395

Source: Calculated by the author based on data from Nasdaq Baltic Stock Exchanges Home Page (n.d.) and Markets Data - Stock Market, Bond, Equity, Commodity Prices - FT.Com (n.d.).

In summary, the cross sectional patterns show considerable variation between categories despite the absence of statistical significance. Industries with higher digital exposure, incidents involving criminal actors and attacks targeting data tend to show consistent and more negative CARs. In contrast, events attributed to non-criminal factors and denial of service attacks show small positive or close to zero effects. These patterns display markets' short term reaction to a cyber incident can depend on the nature of the attack. Although the sample size limits the strength of these conclusions, the results show some cyber incidents generate heterogeneous market responses that are not visible in the AR averages.

3.4 Qualitative assessment of firm responses to cybersecurity incidents

The following step for the analysis is to examine how firms communicate and manage cybersecurity incidents by reviewing publicly available disclosures issued after each event. The purpose is to complement the event study and evaluate whether differences in communication practices, governance actions or post incident Investments decisions help explain variation and market reactions, and provide indications of how incidents influence future financial and risk management decisions of the company.

In several cases, the incident was first reported not by the company, but hacker groups or other actors, and companies themselves did not confirm or publicly acknowledge the possible event. Reasoning for such cases can be various - some threat actors might be exaggerating the scale of an incident or try to intimidate the company. In other cases companies might investigate the case and find no serious impact, no systems compromised, or that the incident had no operational or financial impact which would legally require disclosure. Following that, companies choosing not to communicate the incident does not necessarily mean the company is withholding information. It can reflect that the incident was minor, impossible to confirm, or private communication was chosen. Since further analysis is built on companies' response to the event, cases where no public information from the company was found on the event were not evaluated and used in further qualitative analysis.

Given the differences on how companies communicated the incidents, the qualitative assessment focuses on firms with identifiable event related disclosures. For these cases, sufficient material was sourced to evaluate the response in terms of predefined categories. For companies that issued no statement or only very limited information, the analysis records this as N/A and no further assessment is possible. The following part presents short summaries for each firm. Each summary reviews the event communication based on categories and provides background to the Tables 11 and 12, where evaluation is provided.

The companies and events accordingly can be split to two groups, one where the company officially issues a statement, and another group where the company only responds to questions raised by media outlets, but does not have an initial announcement or a report later. Table 11 covers 5 companies with no official announcement, Table 12 covers companies with official announcements. In the table, “Strong” indicates a strong company's response in that category, “Partial” means it was provided but not in great detail, “N/A” means the category was not addressed in the analyzed source.

Table 11

Evaluation of companies with no official statements based on the events.

ID	Company	Source	Timing	Remediation	Investment	Governance	Communication
1	CD Projekt Red	Company form posts (removed), email days after announcement	Partial	N/A	N/A	N/A	Partial
5	Ericsson	News report	N/A	N/A	N/A	N/A	N/A
22	Nokia	Response to a company	N/A	N/A	N/A	N/A	Partial
28	Pandora	News report	N/A	Strong	N/A	Yes	Strong
29	DSV	News report	Yes	Strong	N/A	Yes	Partial

Source: (Araújo et al., 2022; China Hacked 8 Major Technology Firms in Elaborate 'Cloud Hopper' Attack: Report - National | Globalnews.Ca, 2019a; Game Studio Behind Witcher 3 Held for Ransom Over Stolen Files, n.d.; Hackers Claim Access to Nokia Internal Data, Selling for $20,000 – Hackread – Cybersecurity News, Data Breaches, AI, and More, 2024; Radauskas, 2025)

CD Projekt Red (Event ID 1) incident was reported on 2017 January 31st. The incident was first reported by external media sources that confirmed the breach compromised approximately 1.8 million user accounts. The company did not publish a formal press release or regulatory statement to the event. Users were informed by email days after the reports made by media sources, other communication appeared only through posts on companies' forums, which were informal and later removed (*Game Studio Behind Witcher 3 Held for Ransom Over Stolen Files*, 2017). No detailed technical explanation or scope of the breach was provided. The firm also did not provide information on remediation actions or any cybersecurity improvements in its annual reports. Overall the communication was limited - poor timing, content and structure. Absence of formal documentation shows low level of transparency.

The event involving Ericsson (Event ID 5) was reported through multiple external news sources in December of 2018, while the company did not issue any public statement acknowledging the attack (*China Hacked 8 Major Technology Firms in Elaborate 'Cloud Hopper' Attack: Report - National | Globalnews.Ca*, 2019). The reports describe a multi year cyber attack on multiple companieS, Ericsson being one of them, but Ericsson provided no confirmation,

clarification or investigation statements. There was no communication on timing, remediation or internal response measures. The incident was not mentioned in the annual reporting or investor communications. In the absence of any official disclosure, it is not possible to evaluate the companies' governance or disclosure practices. This displays lack of communication or poor strategy of Ericsson.

Nokia's case in 2024 November started as a claim by hackers, that the companies' data was accessed, and attempted to sell for 200,000USD. Data allegedly included sensitive development assets and credentials. Nokia issued no official statement regarding the incident, but responded to news outlets requests to comment, saying they are actively investigating the claim, but state they have no verification compromise of the systems or on customer data (*Hackers Claim Access to Nokia Internal Data, Selling for $20,000 – Hackread – Cybersecurity News, Data Breaches, AI, and More*, 2024). Multiple IT news outlets received the same answer, but no statement confirming or denying the breach was issued. Apart from the short response, Nokia did not disclose any information on remediation or governance changes, no references to the event at the annual report. As a result, Nokia's communication remains minimal and reactive, focusing on correcting misinformation.

Pandora (Event ID 28) confirmed that customer data was accessed through a compromised third-party platform in July of 2025. Internal systems were not accessed, but basic data of names and email addresses was involved. Pandora sent out emails as an announcement after the incident was contained, no sensitive or financial data was affected. Other than emails, no official public statements have been made other than responding to news outlets' questions. Customers were advised to be aware of phishing attempts (Radauskas, 2025). Pandora did not disclose exact timing of the breach, remediation is confirmed through containment of the incident, strengthened security and ongoing monitoring. No related investment decisions or cybersecurity tools were named, the incident was not mentioned in the annual reports. Governance in terms of cybersecurity seems not well developed. Communication strategy was private, limited in scope.

DSV (Event ID 29) in October of 2025 confirmed investigating a data breach involving smaller customer platforms after a hacker group claimed responsibility. The company stated that the affected platform has been isolated, external experts are assisting, and show no proof of impact on core systems. Only a limited number of customers were affected and were notified directly. DSV declined to disclose additional information for the website and did not make an announcement on their end (Araújo et al., 2022) The timing of the event is stated in the article. Remediation is demonstrated through platform isolation, external support and investigation. The

company does not provide information for the news outlet on investments or new spending on security upgrades. Governance is displayed by structured communication for the media and informing affected customers personally. Communication is confirmed through controlled information given to the media and notifying customers.

The following companies issued public official statements regarding the reported incident. These disclosures allow for more even assessment between the announcements. Table 12 below summarizes the communication characteristics for this group.

Sandvik (Event ID 2) was affected in May 2017 - global virus attack that disrupted operations for several industrial firms. The company issued an official public announcement for the incident, confirming that its systems had been restored (*Sandvik's Comment on the Global Virus Attack*, 2017). The initial announcement is direct and early, acknowledging the operational impact of the incident and actions taken for recovery. The incident was then addressed in the annual report, but it did not cover details or subsequent cybersecurity measures, only general investment into IT (*SANDVIK ANNUAL REPORT 2017*, n.d.). Across these documents, the response was strategic and informative, but no details on cyber investment decisions or governance in case of a cyber event were provided. The communication was limited in terms of how internal processes were explained or how their future risk management would change, but remained strategic.

CD Projekt Red (Event ID 3) went through another public attack in June of 2017. This time the company posted a short message on X (formerly Twitter) informing of a ransom demand on stolen files (*CD PROJEKT RED on X*: "Https://T.Co/EP2OatjZZW" / X, 2017). The company stated that they have refused to comply with the demands and warned users about potential risks. Operational impact has not been covered, also there has been no reference to the event in the annual reports of 2017. No information on investment in cybersecurity or change in governance structure has been provided. Overall, the companies' response was limited, but improved drastically compared to the attack the company experienced in previously the same year.

Maersk (Event ID 4) Issued an official public statement saying that the company was struck by a malware attack in June of 2017. The announcement was investor oriented, clear. it explained the attack, operational disruptions that occurred and provided remediation steps. the statement was updated with progress when the systems were restored (*Cyber Attack Update | A.P. Møller - Mærsk A/S*, 2017). The company's annual report summarized the operational impact and recovery process of the incident providing more details (*MAERSK 2017 Annual Report*, 2017). The company also issued a risk management documentation that also

mentioned the event, provided context to the attack, described losses and recovery from the incident, and explained extensive mitigation actions that were taken. Immediate and long-term cyber resilience measures were implemented by the company, recovery capabilitiesIncreased and cyber insurance has been purchased (*MAERSK 2017 Risk Management*, 2017). Considering all three documents, the company can be evaluated strongly. Communication was extensive, in a timely manner, the scale of the incident was explained and with structural explanations. This type of communication covers key points and shows a high level of transparency.The incident influenced operational decisions of the company, planning and risk management was influenced by the event, and overall governance was affected by the event, yielding positive change.

Norsk Hydro experienced a major ransomware attack in March 2019, that forced the company to shift to manual operations for the time of the attack. The company released an official announcement describing the attack, confirmed cooperation with external experts and authorities and also provided the public with information on immediate operational consequences (*Cyber-Attack on Hydro | Hydro*, n.d.). Hydro continued to issue updates over the following days after the incident. The statements included explanations of affected systems and progress in restoring operations. The communication remained well structured but focused on facts, service continuity and the safety of internal systems. The company covered cyber insurance and maintained regular contact with stakeholders through the course of the incident. Hydro's communication was very transparent and well detailed.

AKVA in January of 2021 announced in an official public statement that the company was a target of a cyberattack that disturbed multiple key systems. The company stated that they worked with Norwegian authorities and external partners to assess the situation and contain the attack. AKVA had not determined the full impact or provided an expected resolution time at the time of the announcement (*AKVA Group ASA: Hit by Cyber-Attack - AKVA Group*, 2021). Annual report confirmed the severe cyber attack, stating that it required substantial management, and that restoration took up half a year. The financial statements stated 43.4NOK million in cyber expenses. No details on data loss were disclosed, but the report covers management of the event and the impact of the attack (*Annual Report AKVA Group 2021*, n.d.). The company's communication was clear and concise, provided a timeline and remediation details. Governance procedures were displayed in management's involvement in handling the crisis and formal reporting on the attacks. Communication strategy seems to be well planned as seen in instant coverage and annual financial reports, but not very high in transparency.

CD Projekt Red (Event ID 8) experienced yet another attack in February 2021. The company confirmed a targeted attack compromising internal systems on X, saying that some servers were encrypted, but backups remained intact (*CD PROJEKT RED on X*: “Important Update Https://T.Co/PCEuhAJosR” / X, 2021). A ransom note was left by attackers but the company refused to negotiate. The company provided statements on secured infrastructure, started restoration and confirmed no personal data has been affected. Annual reports did not mention cybersecurity governance or investment in this area. The company also put attention on transparency and ongoing investigation of the event. The statement shows strong strategic response, providing details, restoring data. The attack was discovered a day prior to the announcement, and had formal incident response - communication seems timely and detailed. A responsive governance system seems to be in place - CD Projekt Red stated they are working with authorities and IT forensic specialists.

Ignitis Group reported the strongest cyberattack in a decade that disrupted websites and electronic services in July of 2022 (*Ignitis Grupė - Ignitis Grupė Susiduria Su Didžiausia...* | *Facebook*, 2022). They addressed coordination with national cybersecurity authorities and implemented immediate actions to restore digital services. The attack affected public services but did not compromise infrastructure or customer data. In the annual report of the year of the incident, the group took preventative measures to manage increased cyber risks, strengthened cooperation with internet service providers, and invested in cloud-based protection. Disclosure was made real time with an announcement issued in the morning after the overnight attack. Additional investment into cloud protection was set to defend against DDoS, CERT accreditation and strengthened governance processes (*Ignitis Group 2022 Annual Report*, n.d.). The group demonstrated timely disclosure of the event, strong operational continuity, and described long term risk management. Immediate cooperation with national cybersecurity and clear reporting also indicates strong, formal governance structure.

REC Silicon (Event ID 18) reported its cyber incident in December 2022 through a press release. The company stated that data had been stolen and leaked (*REC Silicon - Cyber Security Incident (Press Release)*, 2022). The announcement confirmed the alleged breach, and informed the public that business operations have not been significantly disturbed. It did not provide details on the remediation. The incident was later referenced in the company's 2022 annual report, which confirmed the attack and briefly outlined cybersecurity risks (*2022 Annual Report REC Silicon*, n.d.). REC Silicon offered clear communication of the incident itself confirming timing and impact but further detail on investments or governance changes was

absent. Transparency was moderate because the firm confirmed the breach, but provided limited information beyond the immediate security statement and summary in the annual report.

TOMRA (Event ID 20) experienced a major attack in July of 2023 forcing the company to disconnect systems, deploy manual processes, and activate incident response teams. TOMRA issued continuous public updates while restoring operations (*TOMRA July 20th Update on Cyberattack*, 2023). The company implemented extensive security enhancements. The annual report covered the incident, plans to strengthen security measures and increase the amount of internal controls and focus on better risk management (*TOMRA Annual Report 2023*, n.d.). Overall, TOMRA provides specific timing of the attack and restoration. Remediation strategy is clear because of system disconnections, rebuilding digital services, investigating the event and other measures that were described in the updates and initial statements. Multiple security frameworks and platforms were introduced, confirming investment in security. The company worked with authorities, coordinated internal and external teams to manage the event, and followed formal communication protocols. This shows strong governance systems within the company. Communication is clear and detailed.

In 5 cases out of the sample of 28 events, the companies did not issue an official statement. Looking at each case, some of those that did not issue an official statement, included cases with large data breaches, and some were events that were never confirmed by the company. These companies relied on indirect communication channels, like responses to media inquiries, customer emails, or informal posts. In these cases, disclosure was often delayed, limited, or reactive. For 9 events, official statements were issued. Companies issued official statements and generally provided clearer timelines, information on operational impact as well as remediation actions.

Across all companies, communication most frequently focused on operations. Many statements emphasized system restoration, service availability, and fixing of customer data compromise. Remediation actions like system isolation, external forensic support, or cooperation with authorities were also commonly mentioned. However, discussion of long term cybersecurity investments or improving governance structures to manage cyber events were less frequent. Even within companies that had well structured communication, references to new security spending or oversight and strategic risk management adjustments were brief or not addressed.

Table 12

Evaluation of companies that issued official statements based on the events.

ID	Company	Source	Timing	Remediation	Investment	Governance	Communication
	Sandvik	Official announcement	Strong	Strong	N/A	N/A	Partial
2	Sandvik	Annual report	N/A	N/A	Partial	Partial	N/A
3	CD Projekt Red	Official announcement	Strong	Partial	N/A	N/A	Partial
	Maersk	Official announcement	Strong	Strong	N/A	Partial	Strong
	Maersk	Annual report	N/A	Partial	Strong	Strong	N/A
4	Maersk	Risk management strategy	N/A	Strong	Strong	Strong	Strong
6	Norsk Hydro	Official announcement	Strong	Strong	Strong	Strong	Strong
	AKVA	Official announcement	Strong	Strong	N/A	Partial	Strong
7	AKVA	Annual report	Strong	Strong	N/A	Strong	Strong
8	CD Projekt Red	Official announcement	Strong	Strong	N/A	Strong	Strong
	Ignitis Group	Official announcement	Strong	Strong	N/A	N/A	Partial
9	Ignitis Group	Annual report	Strong	Strong	Strong	Strong	N/A
	REC Silicon	Official announcement	Strong	Strong	Partial	Strong	Strong
18	REC Silicon	Annual report	Strong	Strong	Strong	Strong	Strong
	Tomra	Official announcement	Strong	Strong	Strong	Strong	Strong
20	Tomra	Annual report	Strong	Strong	Strong	Strong	Strong

Source: (2022 Annual Report REC Silicon, n.d.; AKVA Group ASA: Hit by Cyber-Attack - AKVA Group, 2021a; Annual Report AKVA Group 2021, n.d.-a; CD PROJEKT RED on X: "Https://T.Co/EP2OatjZZW" / X, 2017a; CD PROJEKT RED on X: "Important Update Https://T.Co/PCEuhAJosR" / X, 2021a; Cyber Attack Update | A.P. Møller - Mærsk A/S, 2017;

Cyber-Attack on Hydro | Hydro, n.d.-a; Ignitis Group 2022 Annual Report, n.d.; Ignitis Grupė - Ignitis Grupė Susiduria Su Didžiausia... | Facebook, 2022; MAERSK 2017 Annual Report, 2017a; REC Silicon - Cyber Security Incident (Press Release) , 2022; SANDVIK ANNUAL REPORT 2017, n.d.-a; Sandvik's Comment on the Global Virus Attack, 2017a; TOMRA Annual Report 2023, n.d.-a; TOMRA July 20th Update on Cyberattack , 2023; Møller -Maersk, 2017)

Also a clear difference is observed between initial accident announcements and annual reports. Initial statements disclose the incident, immediate impact and remediation. If mentioned in the annual reports, incidents are covered from risk management or internal control angles. Coverage provides more structured information on governance, risk oversight, and if the investments in cyber security capabilities or insurance were made.

Across all companies, communication most frequently focused on operations. Many statements emphasized system restoration, service availability, and fixing of customer data compromise. Remediation actions, including system isolation, external forensic support, or cooperation with authorities were also commonly mentioned. However, explicit discussion of long term cybersecurity Investments or improving governance structures to manage cyber events were less frequent. Even within firms that had well structured communication, references to new security spending or oversight and strategic risk management adjustments were brief or not addressed. Also a clear difference can be observed between initial accident announcements and information in annual reports. Initial statements disclose the incident, immediate impact and remediation. If mentioned in the annual reports, incidents are covered from risk management or internal control angles. Coverage provides more structured information on governance, risk oversight, and if the investments in cyber security capabilities or insurance were made.

The fourth hypothesis, "Do cybersecurity incidents affect companies' future investment decisions?", is analyzed based on qualitative analysis. As described above, the evidence on how much information is disclosed on what the investments are or will be after the incident, is very limited, with most information if provided by the company, appears later in annual or similar reports. Therefore this hypothesis is also rejected.

Several firms demonstrated structured incident response and coordination with authorities, a few provided specific information on how the incident affected investment decisions, internal risk management frameworks, or long term cost considerations. The companies might be reluctant to disclose their internal governance arrangements, response team structures, or strategic risk management practices to maintain confidentiality or due to security concerns. In many cases cybersecurity was presented as a technical or operational

challenge. Disclosures were often focused on immediate containment and service restoration and reporting the event in annual statements.

Companies mainly report control and operational stability after a cybersecurity incident. Most disclosures focus on restoring services and limiting disruption, suggesting that companies aim to reassure customers and business partners that the incident is contained and temporary. In contrast, information on cybersecurity investments and governance changes is often limited or absent and initial reporting. Transparency on how firms manage cyber risk in the long term remains low. This can increase information as symmetry between investors and the company. In most of the events, cyber incidents are often presented as isolated operational, one-time problems that do not prompt broader changes in the risk management.

3.5 Market reaction differences by cybersecurity response categories

The following section examines how cumulative abnormal returns differ across the companies, based on the qualitative response categories. Differences in previously determined categories and overall response strength may signal companies risk management capabilities. If investors interpret these characteristics as indicators of how effectively the company manages risks, they might be reflected in stock price behavior around the disclosure date. The following analysis therefore will check for connection between qualitative responses and short term market reactions. Below Tables 13, 14, 15, 16 and 17 report CARs across event windows by category. This section tests the second hypothesis that aims to check if market reactions to cyber incidents are systematically different based on incident characteristics.

Table 13 shows all negative CARs across all timing groups and event windows. For event windows 1 and 2 the values are similar across all timing groups. For event window 3, the values are slightly more negative, with lowest being -0.027. Differences across timing categories are limited and do not follow a clear pattern. Strong timely disclosure is not associated with less negative short term market reactions in this case. This suggests that disclosure timing alone does not mitigate immediate investor response.

Table 14 shows mean CARs for Remediation category through event windows. Firms with no remediation actions disclosed show negative CARs across all windows, partial remediation category shows small positive CARs, with this effect disappearing for the third event window, with CARs turning negative again. Remediation strength does not display reduced short-term negative market reactions and appears to reflect incident severity.

Table 15 displays that firms with no disclosed cybersecurity investment actions experience relatively small negative CARs across all windows. Firms reporting partial or strong

cybersecurity investments experience substantially more negative cars especially in the shortest window. This pattern could suggest that disclosed investments are taken as a signal of a severe incident to the company.

Table 13

Mean CARs by disclosure Timing category.

Timing/Window	[-1, +1]	[-2, +2]	[-3, +3]
N/A	-0.018	-0.016	-0.025
Partial	-0.017	-0.018	-0.027
Strong	-0.019	-0.015	-0.027

Source: Calculated by the author based on data from Nasdaq Baltic Stock Exchanges Home Page (n.d.) and Markets Data - Stock Market, Bond, Equity, Commodity Prices - FT.Com (n.d.).

Table 14

Mean CARs by Remediation category.

Remediation	[-1, +1]	[-2, +2]	[-3, +3]
N/A	-0.018	-0.017	-0.026
Partial	0.011	0	-0.02
Strong	-0.022	-0.017	-0.027

Source: Calculated by the author based on data from Nasdaq Baltic Stock Exchanges Home Page (n.d.) and Markets Data - Stock Market, Bond, Equity, Commodity Prices - FT.Com (n.d.).

Table 15

Mean CARs by Investment category.

Investment	[-1, +1]	[-2, +2]	[-3, +3]
N/A	-0.01	-0.011	-0.024
Partial	-0.057	-0.054	-0.039
Strong	-0.059	-0.023	-0.04

Source: Calculated by the author based on data from Nasdaq Baltic Stock Exchanges Home Page (n.d.) and Markets Data - Stock Market, Bond, Equity, Commodity Prices - FT.Com (n.d.).

Table 16 represents the CARs for Governance category. Companies with no disclosed governance response showed slightly negative CARs across all event windows. Partial

governance responses are showing small positive CARs in windows 1 and 2, while strong governance responses have negative CARs across all windows, with values lower than weaker governance responses. This suggests that governance disclosures tend to coincide with more severe incidents, not mitigating short term market reactions.

Table 16

Mean CARs by Governance category.

Governance	[-1, +1]	[-2, +2]	[-3, +3]
N/A	-0.015	-0.016	-0.028
Partial	0.006	0.011	-0.008
Strong	-0.058	-0.038	-0.039

Source: Calculated by the author based on data from Nasdaq Baltic Stock Exchanges Home Page (n.d.) and Markets Data - Stock Market, Bond, Equity, Commodity Prices - FT.Com (n.d.).

Table 17 Reports CARs across event windows grouped by communication quality. Firms classified as having partial communication show the least negative CARs across all three windows. Companies with no communication show moderately negative CARs and firms with strong and detailed communication experience the most negative CARs. This pattern suggests that more extensive communication does not mitigate short term market reactions and may instead make the events be perceived as more severe or disruptive.

Table 17

Mean CARs by Communication category.

Communication	[-1, +1]	[-2, +2]	[-3, +3]
N/A	-0.015	-0.02	-0.02
Partial	-0.006	-0.005	-0.017
Strong	-0.033	-0.027	-0.038

Source: Calculated by the author based on data from Nasdaq Baltic Stock Exchanges Home Page (n.d.) and Markets Data - Stock Market, Bond, Equity, Commodity Prices - FT.Com (n.d.).

Table 18 reports grouped CARs by the summed response score, which captures overall strength of firm response across all qualitative categories, where N/A was 0, Partially was assigned 1 and Strong response was assigned a 2. The summed score is constructed by assigning values to each category and summing them for each firm. Higher values indicate

more extensive and comprehensive responses across dimensions, and lower scores reflect limited or no disclosed response. The three response groups are split by summed score, where Low response group includes events where companies scored between 0 and 3, moderate response group includes scores 3 to 7 and high response group 8 to 10. This grouping reflects increasing levels of communication strategy and more comprehensive company actions after the incident. Here is also where the third hypothesis is tested (Do companies with higher quality communication post-incident experience milder negative market reactions).

The results show that firms with low response strength show moderately negative CARs for all event windows, moderate response strength shows least negative CARs within all categories, especially in the shorter windows, and companies with high response strength have most negative CARs for all the windows. This pattern suggests that extensive responses are associated with more severe incidents and stronger market reactions, without being rewarded by investors for transparency or disclosure quality.

Table 18

Mean CARs of grouped companies on strength of the response.

Response group	[-1, +1]	[-2, +2]	[-3, +3]
Low	-0.018	-0.017	-0.026
Moderate	-0.007	-0.008	-0.023
High	-0.058	-0.038	-0.039

Source: Calculated by the author based on data from Nasdaq Baltic Stock Exchanges Home Page (n.d.) and Markets Data - Stock Market, Bond, Equity, Commodity Prices - FT.Com (n.d.).

Overall the cross-sectional analysis shows that CARs vary across the categories defined in qualitative research, but no category consistently displayed less negative market reactions. Differences in disclosure timing, remediation, investment decisions or governance as well as communication do not show consistent connection to higher or lower CARs. In several cases, stronger and more extensive responses are associated with more negative CARs, indicating that these responses likely reflect incident severity rather than effective risk mitigation. These findings suggest that short term market reactions could be driven by the nature of the cybersecurity incident. The observed results show some differences between categories, but none of the cross-sectional differences are statistically significant across event windows, rejecting the second hypothesis. The third hypothesis is also rejected, because grouped by

response strength, the market reactions for stronger responses did not provide milder negative reactions than the companies that were grouped under low or moderate response strength groups.

3.6 Synthesis and interpretation of the results

The objective of this research was to examine how cybersecurity incidents affect value and companies' risk management on communication practices mitigate these effects and capital markets.

The theoretical analysis consistently demonstrates that cybersecurity now is a more complex financial and strategic issue, evolving from a technical concern. The literature confirms that cybersecurity incidents have an effect on a company's value seen in short term market reactions and later changes in companies governance and strategic changes. Stock prices are shown to decline after the cyber incident announcements, but can vary across incident types, but the effects are more visible especially when the incidents include data exposure, or disrupt business operations. Existing literature also shows how communication and governance after the companies' announcement of the cyber event can signal to investors, shaping their understanding of the events. Some studies show that cyber incidents lead companies to adjust future investment into risk management or cyber resilience, or insurance. These patterns are what the hypotheses are formed upon.

The empirical findings are complex. The event study does not show statistically significant abnormal returns or cumulative abnormal returns on or after the disclosure date at the aggregate level. Based on the analysis, cybersecurity incidents in the sample did not cause a strong short term price change. This result is consistent with the theory analysis that shows that financial markets are anticipating some cyber risk, as it is hard to avoid, but possible to prepare for.

The economic relevance of cyber incidents, even with no aggregate significance found in the sample is present as seen in cross sectional analysis. It shows variation in cumulative abnormal returns across industries, attacker types, and events of types. The incidents that include data compromise, criminal actors, and incidents that occur in sectors of high digital dependence return more negative CARs. Theoretical analysis provides background for this mechanism, showing how investors assess cyber incidents based on the potential impact they might have on cash flow, continuity of operations and reputation overall. Data integrity, long term trust affecting incidents show to cause more volatile reactions in the markets. Incidents that just cause temporary service disruptions are less likely to cause an intense reaction.

Insignificant aggregate market reactions can be partially explained by qualitative analysis. As seen by the qualitative analysis, company disclosures typically frame cybersecurity incidents as simply operational disruptions. Initial announcements focus on containment, restoration of services and reassurance to customers and partners. References to governance reforms, cybersecurity investments, or changes in internal risk management structures are limited, especially in real time disclosures or announcements of the cyber event. If and when this information is this closed it mostly appears later, in annual reports and is presented in broad and non-incident specific terms.

This reporting pattern has important implications for information asymmetry. From a theoretical perspective, transparency and governance disclosure should reduce uncertainty and support investor confidence. In practice, companies provide limited information about future plans on how cybersecurity incidents affect long-term investment decisions or management. The companies might be reluctant to disclose their internal governance arrangements, response team structures, or strategic risk management practices to maintain confidentiality or due to security concerns. As a result of this investors may lack information needed to assess specific cyber risk exposures or future costs. This partially explains why the disclosure quality does not translate into immediate positive market reactions.

The cross-sectional analysis of CARs by qualitative response categories provides more background. Firms with stronger and more comprehensive responses do not experience less negative CARs, and in several cases, firms with extensive communication, remediation, and governance disclosures show more negative market reactions. This analysis therefore suggests that the very detailed, strong responses are interpreted by the market as signs of severe cyberincident. Disclosures that reveal how costly the incident or breach was, or provide extensive responses shows that companies are signaling the seriousness of the incident and increase attention from the investors to the breach. Because there is little regulation on disclosure requirements, these announcements can be perceived in such a manner.

Effective cyber security governance and investments are expected to reduce long term risk. On the other hand, disclosing them does not provide immediate reassurance to investors after the cyber incident. Based on existing evidence, markets seem to take into account expected losses, anticipating them in a certain way, with the quality of firm response being less important. Cybersecurity risk management may in return influence companies' value through long term strategy, such as sustained investment, improved controls, or reduced probability of future incidence.

The results also contribute to the context of investment behavior following cybersecurity qualitative evidence shows that specific references to cybersecurity Investments are relatively rare and initial disclosures. If the investments are mentioned, they serve as a response to specific incidents and not a strategic change. Empirically, firms that disclose cybersecurity investments show more negative CARs, suggesting that such disclosures are associated with more severe incidents.

From a corporate finance perspective, the findings suggest that cybersecurity risk is not fully incorporated into short-term valuation adjustments. Investors seem to treat cyber incidence as temporary shocks, unless evidence suggests long term financial consequences. Changes And the cost of capital or investment behavior are not immediately reflected in stock prices.

Overall, the empirical results address the research problem and hypotheses raised earlier:

H1: Do cybersecurity incidents lead to significant abnormal returns for affected companies after a cyber incident? Rejected. Neither abnormal returns (ARs) or cumulative abnormal returns (CARs) are statistically significant across any event window. Mean ARs fluctuate around zero with no significant t-statistics. Mean CARs are negative but small, and one sample t-tests fail to reject the null hypothesis across all windows. This indicates no systematic short-term market reaction at the aggregate level.

H2: Are market reactions to cyber incidents systematically different based on incident characteristics? Rejected. Cross-sectional analysis shows consistent directional differences in CARs across industries, attacker types, and event subtypes. Even though specific types of cyber attack types display more negative CARs across all windows, none of the differences reach statistical significance likely due to small sample size.

H3: Do companies with higher quality communication post-incident experience milder negative market reactions? Rejected. Grouping firms by disclosure timing, remediation strength, governance, communication quality, and overall response strength shows no evidence that stronger responses are associated with less negative CARs. In several cases, firms with stronger or more comprehensive responses experience more negative CARs. This suggests that markets interpret extensive disclosure as a signal of incident severity.

H4: Do cybersecurity incidents affect companies' future investment decisions? Rejected. Qualitative evidence shows limited discourse of post incident cybersecurity Investments and initial announcements. When investment is discussed it mainly appears in annual reports and is framed broadly rather than incident specific. Although quantitatively, disclosures related to

Investments are associated with more negative CARs, this information most likely indicates incident severity rather than the reduced risk.

Cybersecurity incidents are financially relevant and increasingly frequent; their short term impact on firm value is limited and heterogeneous. Communication and risk management practices do not mitigate immediate market reactions and suggest that current disclosure practices are insufficient to reduce uncertainty in capital markets.

This section synthesizes quantitative and qualitative findings and shows that cybersecurity incidents did not generate strong or short term market reactions on average, and companies' response characteristics did not reduce immediate valuation effects, based on the data sample. The results show a disconnect between theoretical expectations regarding risk management signaling and observed investor behavior. This suggests that cybersecurity risk management may influence firm value mainly through long term mechanisms.

CONCLUSIONS AND RECOMMENDATIONS

1. The first objective was completed by reviewing and synthesizing the theory on the topic. Cybersecurity risk has become a financially relevant component of corporate risk management, but its short term valuation effects are not uniform. The theoretical review confirms that cybersecurity incidents impose multiple types of costs on firms, including operational disruption, reputational damage, regulatory exposure and long term uncertainty that can affect investment and financing decisions. Cyber risk is integrated into corporate governance, regulatory compliance and enterprise risk management frameworks.
2. The second objective was completed by developing a combining quantitative methodology, using event study method and qualitative methodology, assessing public documents for each company's response and coverage of the cyber events.
3. The third objective was completed by applying the developed methodology to the selected sample. The results show that aggregate market reactions to cybersecurity incidents are limited, but cross-sectional differences provide some information. The event study results do not reveal statistically significant abnormal or cumulative abnormal returns at the aggregate level around the cyber events disclosure dates at the sample level. However, cross-sectional analysis identifies some systematic directional differences across industries, attacker types and event subtypes. Incidents involving data compromise or attributed to criminal activity are associated with more negative

abnormal returns. These findings suggest that investors react to incident characteristics and perceived economic impact, even with average market reactions staying weak.

4. Disclosure timing and communication quality do not reduce short-term valuation effects. The combined quantitative and qualitative evidence indicates that stronger, timelier or in general more detailed disclosures are not associated with milder short term market reactions. In several cases, firms with more extensive communication and remediation efforts experience more negative CARs. This pattern suggests that disclosure quality is a response to the size of a breach or indicates severity. This also shows that disclosure quality by itself does not lead to reduced immediate valuation effects.
5. Even when formal disclosure requirements are in place, information asymmetry is present. The regulatory frameworks are being updated to include more thorough cybersecurity related disclosures, but companies are not yet required to provide real time updates on long term financial implications, governance changes or future investment plans. The disclosure remains selective, creating a disbalance between a company and stakeholders, limiting their ability to assess the company's cyber risk exposure, resilience or potential financial costs.
6. Cybersecurity risk management becomes more relevant in long term planning and strategy adjustments, including investment and risk exposure. Weak response in short term market reaction does not mean that cybersecurity risk is insignificant, the consequences of such events are visible later. These findings suggest that the cybersecurity risk management strategy changes are more likely to happen through long term planning, such as adjusted Investment, better regulatory compliance, governance changes, and related exposure to incidents within the industry, and are discussed, in some cases, in the annual reports. These effects are not captured within short event windows but are important to corporate decision making.
7. Cybersecurity incidents are largely presented by firms as one-time operational disruptions, not ongoing financial risk events. Disclosures focus on service restoration and business continuity, and governance changes, investments into cybersecurity or risk management adjustments are rarely addressed in the initial announcements. This pattern indicates that firms rate incidents as isolated operational shocks that do not trigger immediate strategy reassessments.
8. The last objective, which was interpreting the results in context of corporate finance theory, was also completed. The findings address the research problem by showing that cybersecurity incidents are financially relevant, but the empirical results do not provide

evidence that variation in disclosure timing, communication intensity, or overall response strength is associated with statistically significant differences in short term abnormal cumulative returns. This indicates a gap between theoretical expectations of risk signaling and observed investor behavior.

9. Future research should focus on longer term financial effects of cybersecurity incidents. Short term event windows may not capture changes in investment behaviour, investments or cost of capital. Future studies should examine long term effects, companies' performance, investment decisions and cyber risk management frameworks.
10. Larger data samples should be used to improve statistical significance. The limited sample size constrain the analysis and make it less likely to find statistical significance. Expanding dataset across regions or industries may allow for more robust analysis.
11. Quantified severity of the incident should be incorporated into the future research. Future research should incorporate objective factors that would evaluate the severity of the event, such as quantified financial loss, regulatory fines or volume of compromised data, so that the changes in companies stock price could be analyzed in terms of the size of the severity, rather than relying on categorical classifications.
12. Recommendations for corporate managers and financial executives: cybersecurity risk could be more explicitly integrated into financial risk reporting and investment narratives. Firms may benefit from linking cybersecurity incidents and response measures to capital allocation decisions, risk provisioning, insurance coverage. With a growing dependence on digitality, companies' response on how future incidents should be handled can signal a strong companies cyber awareness and help investor confidence. For this reason, integrating cybersecurity can be beneficial.
13. Recommendation for companies: if operating in digitally intensive or data driven sectors, greater emphasis should be placed on cybersecurity preparation, and transparent post-incident explanation of the scope and containment of the attack. The findings indicate that markets react more harshly to incidents involving personal data compromise, suggesting that companies in these sectors should benefit from proactively communicating data protection strategies and recovery capabilities as a part of their standard risk disclosures, on top of the mandatory coverage.
14. Recommendation for regulators and policy makers responsible for cybersecurity disclosure frameworks: incident reporting requirements should be expanded to include a minimum set of comparable financial and governance indicators at the time of disclosure or within a certain timeframe after the event. These could include whether the incident

triggered unplanned cybersecurity expenditures, changes in risk oversight responsibilities, or revisions of internal frameworks. Introducing such standardized elements would improve comparability across firms, how they handle the incidents. It would also reduce reliance on delayed annual report disclosures and support investor decision making and future empirical cyber research on cybersecurity and financial response of the company.

15. Recommendation for investors: cybersecurity incidents should be evaluated on incident characteristics and company exposure to the risk, and should not be based on the intensity of corporate communication. In order to evaluate companies long term risk management capacity and cost of capital implications, disclosures provided in annual reports should be considered, evaluating investments, risk management frameworks and governance set up for possible cyber incidents or vulnerabilities in the future.
16. The conclusions of this study should be considered with caution due to the limited sample size, reliance on publicly disclosed information, and focus on short term market reactions. While the results provide insight into how cybersecurity incidents are perceived by the markets, they do not capture long term financial effects or undisclosed to public risk management changes.

REFERENCES

2022 Annual report REC Silicon. (n.d.).

Agarwal, N., Agarwal, S., & Chatterjee, C. (2024). Data breach notification laws and the cost of private debt. *The British Accounting Review*, 101518. https://doi.org/10.1016/J.BAR.2024.101518

Akva Group ASA, AKVA:OSL historical prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=AKVA:OSL

AKVA group ASA: Hit by cyber-attack - AKVA group. (2021). https://www.akvagroup.com/investors/the-share/stock-exchange-announcements/akva-group-asa-hit-by-cyber-attack

Ampel, B. M., Samtani, S., Zhu, H., Chen, H., & Nunamaker, J. F. (2024). Improving Threat Mitigation Through a Cybersecurity Risk Management Framework: A Computational Design Science Approach. *Journal of Management Information Systems*, *41*(1), 236–265. https://doi.org/10.1080/07421222.2023.2301178

Annual Report AKVA group 2021. (n.d.).

AP Moeller - Maersk A/S, MAERSK B:CPH historical prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=MAERSK%20B:CPH

Araújo, A., Nathália, I., Vieira, U., Nayara, J., da Silva, F., Pereira De Faria, S., Lorenzoni Nunes, G., Khouri, A. G., Paulo, Á., Souza, S., Cristina De Morais, M., Augusto, A., & Silveira, D. A. (2022). Spaceflight Associated Neuro-ocular Syndrome (SANS): Clinical Update. *Revista Médica Del Instituto Mexicano Del Seguro Social*, *44*(5), 433–440. https://ing.dk/artikel/danish-transport-giant-hacking-mystery-we-are-investigating-data-breach

Assa Abloy AB, ASSA B:STO summary - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/summary?s=ASSA%20B:STO

Asseco Poland SA, ACP:WSE historical prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=ACP:WSE

Balboni, P. D. P., & Francis, K. E. (2025). Data ethics and digital sustainability: Bridging legal data protection compliance and ESG for a responsible data-driven future. *Journal of Responsible Technology*, *22*, 100099. https://doi.org/10.1016/J.JRT.2024.100099

Benton, M., & Radziwill, N. (2017). Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management. *Software Quality Professional*, *19*(4), 25–43.

https://openurl.ebsco.com/contentitem/aci:125076230?sid=ebsco:plink:crawler&id=ebsco:aci:125076230&crl=c

Boggini, C. (2024). Reporting cybersecurity to stakeholders: A review of CSRD and the EU cyber legal framework. *Computer Law & Security Review*, *53*, 105987. https://doi.org/10.1016/J.CLSR.2024.105987

Bruno, E., Pistolesi, F., & Teti, E. (2025). Cybersecurity policy, ESG and operational risk: A Virtuous relationship to improve banks' performance. *International Review of Economics & Finance*, *99*, 104053. https://doi.org/10.1016/J.IREF.2025.104053

Caluwe, L., Wilkin, C. L., de Haes, S., & Huygh, T. (2024). Board roles required for IT governance to become an integral component of corporate governance. *International Journal of Accounting Information Systems*, *54*, 100694. https://doi.org/10.1016/J.ACCINF.2024.100694

Cao, H., Phan, H. v., & Silveri, S. (2024). Data breach disclosures and stock price crash risk: Evidence from data breach notification laws. *International Review of Financial Analysis*, *93*, 103164. https://doi.org/10.1016/J.IRFA.2024.103164

CD PROJEKT RED on X: "https://t.co/eP2OatjZZW" / X. (2017). https://x.com/CDPROJEKTRED/status/872840969795899394

CD PROJEKT RED on X: "Important Update https://t.co/PCEuhAJosR" / X. (2021). https://x.com/CDPROJEKTRED/status/1359048125403590660

CD Projekt SA, CDR:WSE historical prices - FT.com. (n.d.-a). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=CDR:WSE

CD Projekt SA, CDR:WSE historical prices - FT.com. (n.d.-b). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=CDR:WSE

Cheng, S., Li, J., Luo, L., & Zhu, Y. (2024). Cybersecurity governance and digital finance: Evidence from sovereign states. *Finance Research Letters*, *65*, 105533. https://doi.org/10.1016/J.FRL.2024.105533

China hacked 8 major technology firms in elaborate 'Cloud Hopper' attack: report - National | Globalnews.ca. (2019). https://globalnews.ca/news/5432525/china-cyberattack-computer-services-cloud-hopper/

Choi, B. M., Degryse, H., & Smedts, K. (2025). Do Lenders Price Firms' Cybersecurity Risks? *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.5284102

Clausmeier, D. (2022). Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). *International Cybersecurity Law Review 2022 4:1*, *4*(1), 79–90. https://doi.org/10.1365/S43439-022-00076-5

Contact - Spotify. (n.d.). Retrieved November 26, 2025, from https://www.spotify.com/us/about-us/contact/

Corporate sustainability reporting - European Commission. (n.d.). Retrieved September 15, 2025, from https://finance.ec.europa.eu/capital-markets-union-and-financial-markets/company-reporting-and-auditing/company-reporting/corporate-sustainability-reporting_en

Cyber attack update | A.P. Møller - Mærsk A/S. (2017). https://investor.maersk.com/news-releases/news-release-details/cyber-attack-update

Cyber Trends and Credit Risks. (2022).

Cyber-attack on Hydro | Hydro. (n.d.). Retrieved December 17, 2025, from https://www.hydro.com/en/global/media/on-the-agenda/cyber-attack/

Cybersecurity and financial reporting risk: PwC. (2025). https://www.pwc.com/us/en/tech-effect/cybersecurity/mitigating-cybersecurity-financial-reporting-risk.html

Day, K., & Booker, Q. (2024). *Issues in Information Systems Market Reactions to Cybersecurity Incidents: A Case Study Approach*. *25*(4), 260–276. https://doi.org/10.48009/4_iis_2024_121

DelfinGroup | Trading — Nasdaq Baltic. (n.d.). Retrieved January 5, 2026, from https://nasdaqbaltic.com/statistics/en/instrument/LV0000101806/trading

Demek, K. C., & Kaplan, S. E. (2023). Cybersecurity breaches and investors' interest in the firm as an investment. *International Journal of Accounting Information Systems*, *49*, 100616. https://doi.org/10.1016/J.ACCINF.2023.100616

Digital Operational Resilience Act (DORA) - EIOPA. (n.d.). Retrieved September 16, 2025, from https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

DSV A/S, DSV:CPH historical prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=DSV:CPH

Eezy Oyj, EEZY:HEX historical prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=EEZY:HEX

Elmawazini, K., Saadi, S., Sassi, S., Khiyar, K. A., & Ali, M. (2023). Do data breach disclosure laws matter to shareholder risk? *Finance Research Letters*, *53*, 103588. https://doi.org/10.1016/J.FRL.2022.103588

Fedele, A., & Roner, C. (2022). Dangerous Games: A Literature Review on Cybersecurity Investments. *Journal of Economic Surveys*, *36*(1), 157–187.

https://openurl.ebsco.com/contentitem/eoh:2002339?sid=ebsco:plink:crawler&id=ebsco:eoh:2002339&crl=c

Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., Islami, L., & Akil, M. (2021). Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of Information Security and Applications*, *61*, 102916. https://doi.org/10.1016/J.JISA.2021.102916

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2022). Cybersecurity Risk. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3725130

Fotis, F. (2024). Economic Impact of Cyber Attacks and Effective Cyber Risk Management Strategies: A light literature review and case study analysis. *Procedia Computer Science*, *251*, 471–478. https://doi.org/10.1016/J.PROCS.2024.11.135

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security*, *121*, 102840. https://doi.org/10.1016/J.COSE.2022.102840

Gallagher, N., & Harry, C. (2023, June 1). *Classifying Cyber Events: A Proposed Taxonomy | Center for International and Security Studies at Maryland*. https://cissm.umd.edu/research-impact/publications/classifying-cyber-events-proposed-taxonomy

Game Studio Behind Witcher 3 Held for Ransom Over Stolen Files. (2017). https://www.bleepingcomputer.com/news/security/game-studio-behind-witcher-3-held-for-ransom-over-stolen-files/

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *Risk Analysis: An International Journal*, *40*(1), 183–199. https://doi.org/10.1111/RISA.12891

Gao, L., Chen, Z., Zhao, W., & Lai, X. (2025). Does cybersecurity regulation reduce corporate data-breach risk? *Finance Research Letters*, *78*, 107171. https://doi.org/10.1016/J.FRL.2025.107171

Global Cybersecurity Outlook 2025 | World Economic Forum. (2025). https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

GPW Main Market - Main Market. (n.d.). Retrieved December 2, 2025, from https://www.gpw.pl/en-home

Grima, S., & Marano, P. (2021). Designing a Model for Testing the Effectiveness of a Regulation: The Case of DORA for Insurance Undertakings. *Risks 2021, Vol. 9, Page 206*, *9*(11), 206. https://doi.org/10.3390/RISKS9110206

HansaMatrix | Trading — Nasdaq Baltic. (n.d.). Retrieved January 5, 2026, from https://nasdaqbaltic.com/statistics/en/instrument/LV0000101590/trading

Havakhor, T., Rahman, M. S., & Zhang, T. (2021). Disclosure of Cybersecurity Investments and the Cost of Capital. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3553470

He Huang, H., & Wang, C. (2021). Do Banks Price Firms' Data Breaches? *THE ACCOUNTING REVIEW American Accounting Association*, *96*(3). https://doi.org/10.2308/TAR-2018-0643

Huygen, L., & Beulen, E. (2025). Cyber shocks: The financial impact of cyber events. *Social Sciences & Humanities Open*, *12*, 101770. https://doi.org/10.1016/J.SSAHO.2025.101770

Ignitis Group 2022 Annual report. (n.d.). Retrieved December 11, 2025, from https://ignitisgrupe.lt/sites/default/files/public/2024-02/Annual_report_2022_0_0_1_en_33.pdf

Ignitis grupė - Ignitis Grupė susiduria su didžiausia... | Facebook. (2022). https://www.facebook.com/IgnitisGrupe/posts/ignitis-grup%C4%97-susiduria-su-did%C5%BEiausia-kibernetine-ataka-per-de%C5%A1imtmet%C4%AF-nuo-%C5%A1ios-/2129311220573690/

Ignitis Grupe AB, IGN1L:VLX historical prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=IGN1L:VLX

Jamilov, R., Rey, H., & Tahoun, A. (2023). *The Anatomy of Cyber Risk*. https://papers.ssrn.com/abstract=4470871

Jensen, M. C., Meckling, W. H., Benston, G., Canes, M., Henderson, D., Leffler, K., Long, J., Smith, C., Thompson, R., Watts, R., & Zimmerman, J. (1976). Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure. *Journal of Financial Economics*, *4*, 305–360. http://hupress.harvard.edu/catalog/JENTHF.html

Jin, J., Li, N., Liu, S., & Khalid Nainar, S. M. (2023). Cyber attacks, discretionary loan loss provisions, and banks' earnings management. *Finance Research Letters*, *54*, 103705. https://doi.org/10.1016/J.FRL.2023.103705

Joshi, C., Slapničar, S., Yang, J., & Ko, R. K. L. (2025). Contrasting the optimal resource allocation to cybersecurity controls and cyber insurance using prospect theory versus

expected utility theory. *Computers & Security*, *154*, 104450. https://doi.org/10.1016/J.COSE.2025.104450

Joswig, T., & Kurz, W. (2025). Empirical Analysis of NIS2 Adoption in EU SMEs: Challenges for Critical Infrastructure in Germany. *Journal of Next-Generation Research 5.0*. https://doi.org/10.70792/JNGR5.0.V1I3.99

Karakasilioti, G. M. P. (2024). *Supporting the Digital Operational Resilience of the Financial Sector: The EU's DORA Digital Operational Resilience Act*.

Kiesow Cortez, E., & Dekker, M. (2022). A Corporate Governance Approach to Cybersecurity Risk Disclosure. *European Journal of Risk Regulation*, *13*(3), 443–463. https://doi.org/10.1017/ERR.2022.10

Knight, R., & Nurse, J. R. C. (2020). A framework for effective corporate communication after cyber security incidents. *Computers & Security*, *99*, 102036. https://doi.org/10.1016/J.COSE.2020.102036

Konchitchki, Y., & O'Leary, D. E. (2011). Event study methodologies in information systems research. *International Journal of Accounting Information Systems*, *12*(2), 99–115. https://doi.org/10.1016/J.ACCINF.2011.01.002

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659–671. https://doi.org/10.1016/J.BUSHOR.2021.02.022

Levy, A., Ritter, L., Vadala, D., & Pospisil, L. (2021). *Credit Risks in the Face of Cyber and Other Emerging Threats*.

Li, Z., & Liao, Q. (2025). To insure or not to insure: How attackers exploit cyber-insurance via game theory. *Computers & Security*, *157*, 104585. https://doi.org/10.1016/J.COSE.2025.104585

Liu, L., & Shao, M. (2025). ESG-Oriented Boards of Directors and Fintech Risk Management. *Finance Research Letters*, 108369. https://doi.org/10.1016/J.FRL.2025.108369

MacKinlay, A. C. (1997). Event Studies in Economics and Finance. *Journal of Economic Literature*, *35*(1), 13–39. http://www.jstor.org/stable/2729691

MAERSK 2017 Annual Report. (2017).

Malliouris, D. D. (2021). *Finance & cyber security: uncovering underlying and consequential costs of security breaches and investments*.

Markets data - stock market, bond, equity, commodity prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/

Melaku, H. M. (2023). Context-Based and Adaptive Cybersecurity Risk Management Framework. *Risks*, *11*(6), 1–22. https://research.ebsco.com/linkprocessor/plink?id=223cc101-b2ef-358c-846c-443b3903f481

Mizrak, F. (2023). Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Pressacademia*. https://doi.org/10.17261/PRESSACADEMIA.2023.1807

Møller -Maersk, A. P. (2017). *MAERSK 2017 Risk management*.

Moussa, F. Z., & Zine-Dine, K. (2025). The impact of cyber-attacks on cybersecurity investment game model. *Chaos, Solitons & Fractals*, *200*, 117040. https://doi.org/10.1016/J.CHAOS.2025.117040

Nasdaq Baltic Stock Exchanges Home Page. (n.d.). Retrieved January 5, 2026, from https://nasdaqbaltic.com/

Nasdaq Global Index Watch. (n.d.). Retrieved December 2, 2025, from https://indexes.nasdaqomx.com/

NIS2 Directive: securing network and information systems | Shaping Europe's digital future. (n.d.). Retrieved August 24, 2025, from https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

NOKIA, NOK1V:HEX historical prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=NOK1V:HEX

Nong, H., Lin, Y., & Zhang, Q. (2025). Cybersecurity policy and corporate R&D investment. *Finance Research Letters*, *75*, 106939. https://doi.org/10.1016/J.FRL.2025.106939

Norsk Hydro ASA, NHY:OSL historical prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=NHY:OSL

Pandora A/S, PNDORA:CPH historical prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=PNDORA:CPH

Panostaja Oyj, PNA1V:HEX historical prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=PNA1V:HEX

PGE Polska Grupa Energetyczna SA, PGE:WSE historical prices - FT.com. (n.d.-a). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=PGE:WSE

PGE Polska Grupa Energetyczna SA, PGE:WSE historical prices - FT.com. (n.d.-b). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=PGE:WSE

Pigola, A., & da Costa, P. R. (2025). Cybersecurity management: an empirical analysis of dynamic capabilities framework for enhancing cybersecurity intelligence. *Information and Computer Security*, *33*(4), 473–498. https://doi.org/10.1108/ICS-08-2024-0185

PKP Cargo SA w restrukturyzacji, PKP:WSE historical prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=PKP:WSE

Radauskas, G. (2025). *Pandora confirms breach, says customer data at risk | Cybernews*. https://cybernews.com/security/pandora-data-breach-cyberattack/

REC Silicon - Cyber Security incident (Press Release) . (2022, December). https://storage.mfn.se/b429712c-632d-4b36-948b-a71324a20351/rec-silicon-cyber-security-incident.pdf

REC Silicon ASA, RECSI:OSL summary - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/summary?s=RECSI:OSL

Rushing, B., Xu, S., & Fairman, A. (2025). From breach to bias: Measuring reputation value and trust recovery after cyber incidents in critical infrastructure. *International Journal of Critical Infrastructure Protection*, *50*, 100787. https://doi.org/10.1016/J.IJCIP.2025.100787

Sandvik AB, SAND:STO historical prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=SAND:STO

SANDVIK ANNUAL REPORT 2017. (n.d.).

Sandvik's comment on the global virus attack. (2017). https://www.home.sandvik/en/news-and-media/news/2017/05/sandviks-comment-on-the-global-virus-attack/

Saveljeva, J., Uvarova, I., Peiseniece, L., Volkova, T., Novicka, J., Polis, G., Kristapsone, S., & Vembris, A. (2025). Cybersecurity for Sustainability: A Path for Strategic Resilience. *2025 IEEE International Conference on Cyber Security and Resilience (CSR)*, 745–752. https://doi.org/10.1109/CSR64739.2025.11129980

SEC.gov | SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies. (2023). https://www.sec.gov/newsroom/press-releases/2023-139

Senarak, C. (2025). Leveraging advanced technologies and strategies for port cyber resilience: Strengthening incident response and recovery. *Transportation Research Interdisciplinary Perspectives*, *34*, 101666. https://doi.org/10.1016/J.TRIP.2025.101666

Shaikh, F. A., & Siponen, M. (2023). Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, *124*, 102974. https://doi.org/10.1016/J.COSE.2022.102974

Sheneman, A. (2017). Cybersecurity Risk and Bank Loan Contracting. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.3406217

Singh, K., Chatterjee, S., Mariani, M., & Wamba, S. F. (2025). Cybersecurity resilience and innovation ecosystems for sustainable business excellence: Examining the dramatic changes in the macroeconomic business environment. *Technovation*, *143*, 103219. https://doi.org/10.1016/J.TECHNOVATION.2025.103219

Spotify Lists on NYSE as SPOT — Spotify. (2018, April 2). https://newsroom.spotify.com/2018-04-02/tomorrow/

Stine, K., Quinn, S., Witte, G., & Gardner, R. K. (2020). *Integrating Cybersecurity and Enterprise Risk Management (ERM)*. https://doi.org/10.6028/NIST.IR.8286

Taaleri Oyj, TAALA:HEX historical prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=TAALA:HEX

Tan, W., Guo, B., & Zhang, Q. (2025). Cybersecurity governance and corporate market value: Perspectives from investor trust and supply chain trust. *Pacific-Basin Finance Journal*, *90*, 102646. https://doi.org/10.1016/J.PACFIN.2024.102646

Tele2 AB, TEL2 B:STO historical prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=TEL2%20B:STO

Telefonaktiebolaget LM Ericsson, ERIC B:STO historical prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=ERIC%20B:STO

Telia Company AB, TELIA:STO historical prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=TELIA:STO

TOMRA Annual Report 2023. (n.d.).

TOMRA July 20th update on cyberattack . (2023, September). https://www.tomra.com/news-and-media/news/2023/tomra-july-20th-update-on-cyberattack

Tomra Systems ASA, TOM:OSL historical prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=TOM:OSL

Tosun, O. K. (2021). Cyber-attacks and stock market activity. *International Review of Financial Analysis*, *76*, 101795. https://doi.org/10.1016/J.IRFA.2021.101795

Valmet Oyj, VALMT:HEX historical prices - FT.com. (n.d.). Retrieved January 5, 2026, from https://markets.ft.com/data/equities/tearsheet/historical?s=VALMT:HEX

Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*, *52*, 105890. https://doi.org/10.1016/J.CLSR.2023.105890

Waqas. (2024). *Hackers Claim Access to Nokia Internal Data, Selling for $20,000 – Hackread – Cybersecurity News, Data Breaches, AI, and More*. https://hackread.com/hackers-claim-access-nokia-internal-data-selling-20k/

Wolford, B. (n.d.). *What is GDPR, the EU's new data protection law? - GDPR.eu*. Retrieved August 24, 2025, from https://gdpr.eu/what-is-gdpr/

Zadeh, A., Lavine, B., Zolbanin, H., & Hopkins, D. (2023). A cybersecurity risk quantification and classification framework for informed risk mitigation decisions. *Decision Analytics Journal*, *9*, 100328. https://doi.org/10.1016/J.DAJOUR.2023.100328

ANNEXES

Annex 1

Event level CARs and event attributes

event_id	CAR_1	CAR_2	CAR_3	event type	event date	actor type	motive
1	-0.01723	-0.01814	-0.02744	Exploitive	2017-01-31	Criminal	Financial
2	-0.03129	-0.02427	-0.03258	Disruptive	2017-05-12	Nation-State	Financial
3	0.010815	8.19E-05	-0.02043	Exploitive	2017-06-08	Criminal	Financial
4	0.05563	0.066439	0.064998	Disruptive	2017-06-27	Nation-State	Sabotage
5	-0.01487	-0.02015	-0.02026	Exploitive	2018-12-20	Nation-State	Industrial-Espionage
6	0.025093	0.024601	0.010318	Disruptive	2019-03-19	Criminal	Financial
7	-0.04315	-0.04457	-0.08157	Disruptive	2021-01-10	Criminal	Financial
8	-0.06411	-0.07823	-0.0973	Disruptive	2021-02-09	Criminal	Financial
9	-0.00489	-0.00242	-0.00443	Disruptive	2022-07-09	Criminal	Protest
10	-0.06039	-0.07355	-0.07355	Disruptive	2022-08-03	Hacktivist	Protest
11	0	-0.02632	-0.0695	Disruptive	2022-08-14	Hacktivist	Protest
13	0.024727	0.002919	0.017306	Disruptive	2022-08-29	Hacktivist	Protest
14	-0.00258	-0.01118	-0.01261	Disruptive	2022-08-29	Hacktivist	Protest
15	0.001146	0.001547	-0.00162	Disruptive	2022-10-08	Hacktivist	Protest
16	0.04208	-0.02953	0.038495	Disruptive	2022-11-05	Hacktivist	Protest
17	0.068979	0.07989	0.103073	Disruptive	2022-11-18	Hacktivist	Protest
18	-0.05695	-0.05439	-0.03861	Mixed	2022-12-11	Criminal	Financial
19	0	-0.03609	-0.05498	Disruptive	2023-01-07	Hacktivist	Protest
20	-0.05888	-0.02258	-0.03954	Mixed	2023-07-16		Criminal
21	0.030916	0.025439	0.035681	Exploitive	2023-07-17	Criminal	Financial
22	-0.02046	-0.0117	-0.02971	Exploitive	2024-11-04	Criminal	Financial
23	0.004086	0.010673	0.012064	Mixed	2025-03-31	Criminal	Financial

24	-0.06699	-0.10678	-0.10806	Exploitive	2025-04-05	Criminal	Financial
25	0.024829	0.038872	0.037125	Disruptive	2025-04-08	Hacktivist	Protest
26	-0.03029	0.082006	0.034902	Disruptive	2025-04-08	Hacktivist	Protest
27	0.063514	0.098075	0.1066	Disruptive	2025-04-08	Hacktivist	Protest
28	-0.00909	-0.00817	0.000453	Exploitive	2025-07-20	Criminal	Financial
29	-0.00093	-0.00269	0.066792	Exploitive	2025-10-20	Criminal	Financial

Source: Calculated from the main dataset (Akva Group ASA, AKVA:OSL Historical Prices - FT.Com, n.d.; AP Moeller - Maersk A/S, MAERSK B:CPH Historical Prices - FT.Com, n.d.; Assa Abloy AB, ASSA B:STO Summary - FT.Com, n.d.; Asseco Poland SA, ACP:WSE Historical Prices - FT.Com, n.d.; CD Projekt SA, CDR:WSE Historical Prices - FT.Com, n.d.; DelfinGroup | Trading — Nasdaq Baltic, n.d.; DSV A/S, DSV:CPH Historical Prices - FT.Com, n.d.; Eezy Oyj, EEZY:HEX Historical Prices - FT.Com, n.d.; HansaMatrix | Trading — Nasdaq Baltic, n.d.; Ignitis Grupe AB, IGN1L:VLX Historical Prices - FT.Com, n.d.; NOKIA, NOK1V:HEX Historical Prices - FT.Com, n.d.; Norsk Hydro ASA, NHY:OSL Historical Prices - FT.Com, n.d.; Pandora A/S, PNDORA:CPH Historical Prices - FT.Com, n.d.; Panostaja Oyj, PNA1V:HEX Historical Prices - FT.Com, n.d.; PGE Polska Grupa Energetyczna SA, PGE:WSE Historical Prices - FT.Com, n.d.-a; PKP Cargo SA w Restrukturyzacji, PKP:WSE Historical Prices - FT.Com, n.d.; REC Silicon ASA, RECSI:OSL Summary - FT.Com, n.d.; Sandvik AB, SAND:STO Historical Prices - FT.Com, n.d.; Taaleri Oyj, TAALA:HEX Historical Prices - FT.Com, n.d.; Tele2 AB, TEL2 B:STO Historical Prices - FT.Com, n.d.; Telefonaktiebolaget LM Ericsson, ERIC B:STO Historical Prices - FT.Com, n.d.; Telia Company AB, TELIA:STO Historical Prices - FT.Com, n.d.; Tomra Systems ASA, TOM:OSL Historical Prices - FT.Com, n.d.; Valmet Oyj, VALMT:HEX Historical Prices - FT.Com, n.d.).

Annex 2

Event alpha and beta coefficients calculated in the analysis

event_id	alpha	beta
1	0.004352	0.549342
2	0.001593	1.347112
3	0.003594	0.78966

4	0.00023	1.399682
5	0.00191	1.063975
6	-0.00169	1.032599
7	0.00367	0.273939
8	-0.00189	1.078494
9	-0.00035	1.113161
10	0.003358	1.018925
11	0.001446	0.996412
13	-0.00034	0.215129
14	0.000861	0.177505
15	-8.8E-06	1.129662
16	-0.00193	0.996376
17	-0.00079	0.1025
18	0.001684	1.007606
19	0.001387	1.083361
20	-0.00058	0.640491
21	0.001251	1.517413
22	0.001821	1.139411
23	-0.00027	1.064486
24	0.003782	0.441599
25	-0.00378	-0.28588
26	0.000141	-0.02609
27	-0.00118	0.406447
28	0.000335	0.494147

29	0.00064	0.802169

Source: Calculated based on the main dataset (Akva Group ASA, AKVA:OSL Historical Prices - FT.Com, n.d.; AP Moeller - Maersk A/S, MAERSK B:CPH Historical Prices - FT.Com, n.d.; Assa Abloy AB, ASSA B:STO Summary - FT.Com, n.d.; Asseco Poland SA, ACP:WSE Historical Prices - FT.Com, n.d.; CD Projekt SA, CDR:WSE Historical Prices - FT.Com, n.d.; DelfinGroup | Trading — Nasdaq Baltic, n.d.; DSV A/S, DSV:CPH Historical Prices - FT.Com, n.d.; Eezy Oyj, EEZY:HEX Historical Prices - FT.Com, n.d.; HansaMatrix | Trading — Nasdaq Baltic, n.d.; Ignitis Grupe AB, IGN1L:VLX Historical Prices - FT.Com, n.d.; NOKIA, NOK1V:HEX Historical Prices - FT.Com, n.d.; Norsk Hydro ASA, NHY:OSL Historical Prices - FT.Com, n.d.; Pandora A/S, PNDORA:CPH Historical Prices - FT.Com, n.d.; Panostaja Oyj, PNA1V:HEX Historical Prices - FT.Com, n.d.; PGE Polska Grupa Energetyczna SA, PGE:WSE Historical Prices - FT.Com, n.d.-a; PKP Cargo SA w Restrukturyzacji, PKP:WSE Historical Prices - FT.Com, n.d.; REC Silicon ASA, RECSI:OSL Summary - FT.Com, n.d.; Sandvik AB, SAND:STO Historical Prices - FT.Com, n.d.; Taaleri Oyj, TAALA:HEX Historical Prices - FT.Com, n.d.; Tele2 AB, TEL2 B:STO Historical Prices - FT.Com, n.d.; Telefonaktiebolaget LM Ericsson, ERIC B:STO Historical Prices - FT.Com, n.d.; Telia Company AB, TELIA:STO Historical Prices - FT.Com, n.d.; Tomra Systems ASA, TOM:OSL Historical Prices - FT.Com, n.d.; Valmet Oyj, VALMT:HEX Historical Prices - FT.Com, n.d.)