Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Economics and Management
Dept. of Industrial Economics and Technology Management

Nina Hoddø Bakås

Looking for Lemons

A Qualitative Study of Cybersecurity Due Diligence in Acquisitions

Master's thesis in NTNU School of Entrepreneurship
Supervisor: Haakon Thue Lie
December 2020

NTNU
Norwegian University of Science and Technology

NTNU SCHOOL of ENTREPRENEURSHIP

Nina Hoddø Bakås

Looking for Lemons

A Qualitative Study of Cybersecurity Due Diligence in Acquisitions

Master's thesis in NTNU School of Entrepreneurship
Supervisor: Haakon Thue Lie
December 2020

Norwegian University of Science and Technology
Faculty of Economics and Management
Dept. of Industrial Economics and Technology Management

NTNU
Norwegian University of
Science and Technology

Abstract

Acquiring a firm is a good strategy for growth, but included is a great deal of risk associated with acquisitions. The companies, therefore, carry out thorough due diligence of the target firm. The investigations and assessments are carried out to get an overview of vulnerabilities, or "lemons," before a possible acquisition. Thorough due diligence processes reduce the risk of the acquisition, or at least the risks will be known before the acquisition decision takes place. The usual due diligence is to review the financial and legal information in the firm, and also often the commercial possibilities in due diligence. Often the most significant risks have been associated with these fields. The companies are looking for potential legal or financial abuse or that the promised commercial prospects are more optimistic than probable.

In the last decades, a new significant risk has also emerged that can lead to losses in several ways - technology and cybersecurity incidents. As companies are increasingly dependent on technology in operations, the risks of hacker attacks or otherwise being exposed to cybersecurity breaches increase correspondingly. Security breaches can put the company out of daily operations for a more extended period, cause high costs to clean up, weaken the firm's reputation, or in some other way, lower the firm's value.

Based on this, the following research questions have been the focus of this study:

- *How does the Bidder assess the Target firm's cybersecurity before giving a bid?*
- *How relevant is the Target firm's level of cybersecurity for the takeover decision?*

This master's thesis looks at to which extent cybersecurity is considered during the due diligence process by acquiring companies when examining acquisition candidate companies.

The study shows that cybersecurity is considered in the due diligence of an acquisition by all companies in the study. However, notable findings are:

- Two of the three companies considered weak cybersecurity as an acquisitional deal breaker.
- The level of cybersecurity does affect the offer price.
- The state of cybersecurity further affects how the acquirer chooses to integrate the acquired company's technological infrastructure, which has a range of implications, including acquisition and integration costs.
- Over the last six years, also the focus on cybersecurity and data privacy has increased significantly.

Through a literature study, a literature gap was discovered in research on the topic. I have conducted a qualitative abductive survey with semi-structured interviews of managers in three major Norwegian companies. Based on this, I have discussed and concluded what is standard in the industries as of today. I have also concluded how the findings affect both the companies that acquire other companies and entrepreneurial companies with a plan to be acquired. In this way, the study contributes to entrepreneurial business development and technology management.

This page is made blank intentionally.

Sammendrag

Å kjøpe opp et selskap kan være en god strategi for vekst, men det er også stor risiko knyttet til oppkjøp og sammenslåing. Virksomhetene gjennomfører derfor grundige undersøkelser av selskapet i forkant, såkalt due diligence. Undersøkelsene og vurderingene gjennomføres for å få oversikt over sårbarheter, eller "lemons" før et mulig oppkjøp. Grundige due diligence prosesser reduserer risikoen ved fusjoneringen eller oppkjøpet eller i det minste så er risikoene kjente før beslutning om oppkjøp skjer. Det vanlige har vært å gjennomgå det finansielle, juridiske og de kommersielle mulighetene i due diligence. Ofte har de største risikoene vært knyttet til disse feltene. Virksomhetene ser etter potensielle juridiske eller finansielle overtramp eller at lovet kommersielle fremtidsutsikter er mer optimistiske enn sannsynlige.
De siste tiårene har det også vokst frem en ny stor risiko som kan føre til tap på flere måter - teknologi og cybersikkerhetsbrudd. Ettersom bedrifter i økende grad er avhengige av teknologi i operasjonell drift økes samtidig faren for hackerangrep eller på annen måte å bli utsatt for brudd på cybersikkerheten. Dette kan sette bedriften ut av daglig drift i lengre tid, gi store kostnader for å rydde opp, svekke omdømmet til bedriften, eller på en annen måte senke verdien til bedriften.

Ut fra dette ble forskningsspørsmålet utformet:

- *Hvordan undersøker kjøper cybersikkerheten til selskapet de vurderer å kjøpe opp?*
- *Hvor relevant er målfirmaets cybersikkerhetsnivå for overtakelsesbeslutningen?*

Denne masteroppgaven ser på hvordan norske selskaper undersøker potensielle selskaper før oppkjøp, og i hvilken grad undersøkelsen inneholder cybersikkerhet. Oppgaven ser på selskapenes generelle fokus på cybersikkerhet og i hvilken grad due diligence inkluderer cybersecurity.

Ved gjennomgang av eksisterende litteratur ble det identifisert et forskningsgap om temaet. Temaet vil være viktig å belyse, og denne masteroppgaven vil kunne bidra til forskningen på due diligence. Jeg har gjort en kvalitativ abductive undersøkelse med semi-strukturerte intervjuer av ledere i tre større norske selskaper. Ut fra dette har jeg vurdert og diskutert i hvilken grad cybersecurity inkluderes i due diligence ved oppkjøp i store norske selskaper, som har oppkjøp som strategi for vekst. Cybersikkerhetsnivået kan både påvirke selskapene som kjøper opp andre selskaper, og entreprenørielle virksomheter med plan om å bli kjøpt opp. Ut fra intervjuer og tilgjengelig litteratur forsøker jeg å finne svar på forskningsspørsmålene. På den måten bidrar studien inn på entreprenøriell forretningsutvikling og teknologiledelse.

Studien viser at selskapene ser på cybersecurity i due diligence-prosessen. Det skjer i varierende grad og resultatene blir vurdert forskjellig. Alle selskapene i studiet gjør due diligence av cybersecurity og resultatene av due diligence har en påvirkning i beslutningen hos alle selskapene. De to største funnene er likevel at funnene i en cybersecurity due diligence i størst grad påvirker hvilken pris de er villig til å gi og hvordan selskapene integreres inn i det nye morselskapet.

Et annet spennende funn i studien er at de siste seks årene har fokuset på cybersikkerhet i selskapsgjennomgangen før oppkjøp økt betydelig. Alle selskapene sier at det har blitt et generelt større fokus på cybersikkerhet og personvern de siste årene. Dette bekreftes fra intervjuene, selskapenes årsrapport, i tillegg til funn i litteraturstudien.

This page is made blank intentionally.

Acknowledgments and Preface

I have written this thesis at the end of the heavy master's program at NTNU School of Entrepreneurship. Applying for this master's program was one of my smartest decisions so far in life.

Firstly, I will thank Haakon Thue Lie, my supervisor, at the Department of Industrial Economics and Technology Management (NTNU), for guidance throughout the process of writing this thesis. He has helped me through the process of writing, with supporting words and well-needed knowledge. Thank you! It has been wonderfully helpful and enjoyable to get to know you.

The motivation was to find a correlation between my two degrees, the Bachelor's degree in Computer Science from the University of Oslo, and the Master of Science in Entrepreneurship from NTNU School of Entrepreneurship. I've also got to look after my interests in cybersecurity and finance.

My master's degree and master's thesis has by no means been a walk in the park, of course. There have been times of adversity and doubt, but I got through it.

I owe a lot of people many thanks. Especially my mom and dad, the other students at NTNU School of Entrepreneurship, and my colleagues in Adall. You are really tolerant and have been helpful in more ways than you know. Most of all, thank you for just being around and being cool!

I'd also like to give a big thanks to Start Norge, the student organization that allowed me to experiment and develop myself, and Start Norge's members. I have learned a lot from you. Lastly, a big thanks to the University of Oslo and the Department of Informatics for giving me some of the hardest challenges in my life, but more importantly, teaching me the value of hard work.

Nina Hoddø Bakås
December 2020
Oslo, Norway

Table of Content

List of Tables

List of Figures

Chapter 1 - Introduction

1.1 Background

For his study of asymmetric information and introducing the concept of "lemons," George Akerlof received the Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel in 2001 (Nobel Media AB, 2020). He used an example of asymmetric information in the process of buying and selling cars, where "bad cars" are considered as "lemons."

> *"The example of used cars captures the essence of the problem. From time to time, one hears either mention of or surprise at the large price difference between new cars and those which have just left the showroom. The usual lunch table justification for this phenomenon is the pure joy of owning a "new" car. We offer a different explanation. Suppose (for the sake of clarity rather than reality) that there are just four kinds of cars. There are new cars and used cars. There are good cars and bad cars (which in America are known as "lemons"). A new car may be a good car or a lemon, and of course, the same is true of used cars" - Akerlof (1970).*

Akerlof's example of cars can explain the importance of assessing all viable information before purchasing a company to find potential lemons in the target firm. Mergers and acquisitions are some of the largest and most important purchases that are made. Doing these deals, the professionals in the field are well aware of the risks of lemons. Due diligence is spoken of as the most critical process within mergers and acquisitions. Due diligence is mainly done by assessing the information within the target firms' finance and legal operations. It is in these divisions the lemons traditionally are found. They look for lemons as money laundering, bad contracts, or wrongly promised commercial potential. These are still risks or lemons that can cost the acquirer a lot, either in costs, fines, or lower earnings.

A new version of lemons is now in conjunction with data and technology. Technology has made significant business opportunities. Comparing the world's most valuable companies 15 years ago and today shows how data is a valuable resource. Fifteen years ago, oil and gas companies marked the top of the list (Fortune 500, n.d.). In 2020, all the top ten most valuable companies have data as their primary value and technology as their tool (Fortune 500, n.d.). Together with the value follows risk and potential lemons. Data leaks, security incidents, ransomware, and malware are just some examples of lemons, causing trouble for a long time after it occurred.

1.1.1 The Security Incident at Marriott International

The hotel group Marriott International has been dealing with this kind of lemon the last two years, causing a hit on the stock price, a bad reputation, and a large fine from the Information Commissioner's Office (ICO). When Marriott International acquired Starwood in 2016, Marriott knew nothing about Starwood having had a data breach, which had led to data leakage of sensitive information of 339 million customers in 2014. In May 2018, the General Data Protection Regulation came into force, and the security incident was first discovered in the fall of 2018. An unknown attacker stole information, including

emails, names, addresses, passport numbers, and possibly payment card information, in a slow-moving attack that lasted four years (ICO, 2020).

In the summer of 2019, the ICO stated that a £99.2 million initial fine, later changed to £18,4 mill, could be imposed due to Marriott's failures, before its merger with Starwood, to review Starwood's data practices properly and not have done more to secure its systems (ICO, 2019). Elizabeth Denham, Information Commissioner, stated organizations must be accountable for the personal data they hold:

> *"This can include carrying out proper due diligence when making a corporate acquisition, and putting in place proper accountability measures to assess not only what personal data has been acquired, but also how it is protected."*
>
> - *Elizabeth Denham, Information Commissioner (2019)*

And, the case is still not done. GDPR facilitates mass lawsuits from private individuals to companies, and Marriott might still face more considerable fines. These are also only the aftermath given by the ICO. Already in the days after the breach was discovered, investors started asking how Marriott had missed it, and the stock price fastly was down about 5 percent in the days after.

Aware of the security breach two years before the acquisition, the Marriott incident provides an example of the problem and hints to its solutions. A good review of target firms cybersecurity in due diligence before the takeover will continue to be important in the future, as this became particularly important after the GDPR came into force. That Marriott has inherited the responsibility for Starwood's breach sends a clear message to other firms and their future takeovers. Cybersecurity due diligence is a crucial part of any takeover transaction, and the technology, systems, and processes needs to be assessed.

1.1.2 Cyber Lemons

There are also other examples of data lemons with a large impact on a takeover deal. Verizon discounted its initial offer price of Yahoo by $350 million in 2017 after gaining knowledge of two breaches of Yahoo's user data (Shaban, 2017). The medical firm Abbott Laboratories announced the acquisition of St. Jude Medical in 2016 before discovering that St. Jude's had weak cybersecurity, exposing its products to hacking risk a year later (Finkle, 2017). Abbott ended up recalling half a million pacemakers. All three examples have given different outcomes during and after the acquisitions. Marriott was hit by a sizable fine and high cleanup costs, and a bad reputation in the Starwood takeover. Abbott lost earnings and incurred extra charges when they had to recall the pacemakers. While in the deal between Verizon and Yahoo, Yahoo got a discounted offer because the two breaches appeared before the deal was made, and their investors got a lower price for their shares.

The World Economic Forum publishes The Global Risks Report each year, presenting the significant risks the world will be facing in the coming year (World Economic Forum, 2020). In the last four years, Data fraud or theft and Cyberattacks have been ranked higher on both the lists of terms of likelihood and terms of impact, including the top ten and some years the top five risks list.

Cybersecurity has received more attention over the years as the risks have increased. The watch now also comes from the board room, the investors, and the management. A

change from just "some years ago," when cybersecurity was something the "tech guys" should take responsibility for.

Cyber attacks are an increasing risk both in terms of their probability and their impact. Handling and storing of personal information, confidential data, and trade secrets all present risks. Furthermore, the absence of personal information on a targeted system does not make it invulnerable. The uncovering of trade secrets and confidential information can pose an even more significant threat. It can be a direct cause behind lost assets, as seen with business email compromise scams are squeezing more money than ever out of victims, with losses from the attacks almost doubling year-over-year in 2018 to reach $1.2 billion (FBI, 2019). Or it can be a business interruption, as seen after a ransomware attack hit Hydro in 2019, where they lost approximately $55 million (Hydro, 2020).

Studies conducted by Ponemon Institute (2019), CGI and Oxford Economics (2017), and Accenture (2018) have described what an average security incident costs and how security incidents impact the share price. While Accenture (2018) found that the global average cost of cybercrime has risen from $7.2 million in 2013 to $11.7 million in 2017, Ponemon Institute (2019) set an American data incident's average cost at $3,86 million. CGI and Oxford Economics (2017) analyzed data from 65 "severe" and "catastrophic" cybersecurity breaches and found a significant connection between a severe cyber breach and a company's share price performance. It was found that these companies' share prices fell by 1.8% on average on a permanent basis. It was also found that cyber attacks hit the financial services and tech the hardest, and an investor in a typical FTSE 100 company would be worse off by an average of 120 million pounds after a breach.

1.2 Research Question

With Marriott's and Starwood's lessons in mind, it is interesting and important to assess how Norwegian companies do proper cybersecurity due diligence and the impact the cybersecurity due diligence has on the takeover process.

Question 1: *How does the Bidder assess the Target firm's cybersecurity before giving a bid?*

Question 2: *How relevant is the Target firm's level of cybersecurity for the takeover decision?*

1.3 Purpose and Structure

1.3.1 Purpose

The main focus of my bachelor's degree in informatics from the University of Oslo was to gain knowledge in privacy, IT laws, cybersecurity, and IT management. After completing the bachelor's degree, I applied for the master's program at NTNU School of Entrepreneurship. My goals at NTNU School of Entrepreneurship were to learn about technology management and entrepreneurship while building a technology startup within legal-tech and privacy. Some of the courses I have taken as part of my master's degree have been Corporate finance and Digital economy - which both have a focus on how digital transformation changes some of our ways of thinking in the economy. The courses opened my curiosity about this field. The chapter on merger and acquisition in the course Corporate Finance especially woke my entrepreneurial interest from seeing it from an entrepreneur's eyes where doing "an exit" is the long-term goal. This thesis aims to find answers to some of the last requirements for a company before signing the papers for the final meters to be put behind before the finish line on the exit.

With the increased value of data in companies, the company's data's security has also gained importance in due diligence for mergers and acquisitions. The companies have experience with doing due diligence in other areas of the companies, so perhaps they have taken the right processes over to new fields. Therefore, this master's thesis intends to investigate how companies today look at the cybersecurity of the companies they intend to acquire. Furthermore, this study seeks to assess how due diligence for cybersecurity influences the whole merger and acquisition processes even after the decision to merge has been made.

1.3.2 Contribution

In the study of entrepreneurship, this thesis will contribute with knowledge to startups and smaller companies that have an exit goal, including being acquired, which includes most startups. Knowing what larger companies with a strategy of acquiring companies are looking at and assessing when acquiring new firms will provide an advantage for the startup and possibly attain a higher price.

Further, this thesis will also contribute to further research within technology management, giving results in a study that describes how management looks at technology and cybersecurity before acquiring new firms. The thesis also provides some answers about why cybersecurity might be essential to assess before acquiring new firms. This input might help management work with technology, focusing more on cybersecurity in their firm and focusing more on cybersecurity in a takeover process.

1.3.3 Structure

To do the study of how companies assess cybersecurity as part of due diligence in an acquisition process, I have conducted both theoretical and empirical research, followed by an analysis of the collected data. This will serve as the foundation of this thesis. The thesis is structured with the introduction in Chapter 1, where the background for the thesis is presented, the research question introduced, and the purpose explained. In Chapter 2, the theoretical foundation will be presented. This contains a literature review of earlier research and a framework chosen for this study. Chapter 3 presents the study's research method, where I will justify the research method and the case firm

selection. This chapter will also include a discussion about some of the limitations of the research method. Chapter 4 contains individual presentations of the case firms before a multiple case analysis is conducted. Findings from the case firms will be discussed in relation to the theoretical results in Chapter 5, followed by a conclusion of this thesis's key findings in Chapter 6. Lastly, implications and further recommended research will be presented in Chapter 6.2 and 6.3. The interview guide that has been used for the gathering of empirical data is included in the Appendix.

Chapter 2 - Theoretical Foundation

This section presents the theoretical framework that was used as a foundation for the data collection and analysis in this master thesis.
This study explores existing literature to find out what current research says about how technology groups investigate the companies they acquire and how the acquisition process is done.

The literature review is done in the fields of merger and acquisition, and cybersecurity. The subsections look into how the acquisition process goes, what due diligence is, and looks in particular at tech and cybersecurity due diligence. The cybersecurity sub-sections are divided into cybersecurity management and security incidents and the cost of security incidents.

I will also look at this from a perspective on how the literature views this in technology management and in entrepreneurship. And why this is relevant to my study.

In the end of this chapter, I will discuss how I will find a theoretical framework for this study and how this will be used to get conclusions in the end.

2.1 Merger and Acquisition

Merger and acquisitions (M&A) is referred to by Berk and DeMarzo (2017) as being a part of "the market for corporate control". The firm that acquires another is typically referred to as the Acquirer, and the selling firm is called the Target firm." The two primary mechanisms of merger and acquisition, where ownership and control of a corporation changes, is either that the Acquirer acquires the target firm, or the Target firm merges with another firm (Berk & DeMarzo, 2017). In both cases, the Acquirer will purchase the stock or the Target firm's assets for cash or shares of equivalent value. Both mechanisms are referred to as a takeover.

A takeover can be horizontal, vertical, or conglomerate (Berk & DeMarzo, 2017). If the Acquirer and the Target are within the same industry, it is a horizontal merge. If the Acquirer and the Target buy or sell to and from each other's industry, it is called a vertical merge. A conglomerate merger is when the Acquirer and Target operate in unrelated lines of businesses.

2.1.1 The Takeover Process

Berk and DeMarzo (2017) begin explaining the takeover process by establishing how the Acquirer determines the initial offer. The Acquirer will have to value the Target firm and quantify and discount the takeover's value-added result. The valuation of the Target firm can be calculated in several different ways. Some of the most usual might be using a multiple based on comparable firms, as well as an estimate of value. This can also include accurate analysis of the operational aspects as well as the ultimate cash flows the deal will generate (Berk & DeMarzo, 2017). "Once the Acquirer has completed the valuation process, it will make a tender offer - a public announcement of its intention to purchase the Target firm."

An acquisition with a subsequent integration process can be roughly divided into the following phases pre-merger, merger, and post-merger (Hirschheim and Mehta, 2004). Feix (2020) uses the same three phases in his end-to-end merger and acquisition process design, just using the terms embedded merger and acquisition strategy for pre-merger, the transaction management for merger, and integration management for post-merger. This thesis will use Hirschheim and Mehta's terms. According to Aabø-Evensen (2011), the buyer should start planning the post-merger phase, also called the integration process, and test the reality of his assessments already during due diligence, i.e., in the pre-merger phase.

Laws require that when the Target firm's existing shareholders are forced to sell their shares, they shall receive a fair value as compensation (Berk & DeMarzo, 2017). Consequently, Berk & deMarzo (2017) says "Acquirer is unlikely to takeover the Target firm for less than its current market value. Instead, most acquirers pay a substantial acquisition premium, which is the percentage difference between the acquisition price and the target firm's premerger valuation".

In takeovers, it is often seen that a premium is paid in addition to the company's value (Boye & Meyer, 2008). This premium may indicate the reasons for the acquisition. The

reasons for paying a premium on acquisition are expected synergies, over-optimism on the part of the buyer, and desire for expansion. Boye and Meyer (2008) further explain that the acquiring company's management may want expansion, even if this is not profitable. The remuneration, power, and prestige of the management are more dependent on size than profitability (agent costs). Employees may also be interested in the employer diversifying. This can provide safer jobs. Poor management of the Target firm might result in the company being a cheap acquisition candidate. In particular, the synergies are exciting to look at, which may be due to increased revenues, reduced costs, reduced investments, or reduced capital costs.

So, what are the reasons and motives for a takeover? Could the two firms be more valuable together than apart? An Acquirer might add economic value to the Target firm, and by this value, create further synergies (Berk & DeMarzo, 2017). Considerable synergies are by far the most common justification for the Acquirer to takeover the Target firm. Berk and DeMarzo (2017) explain that such synergies usually fall into two categories: cost reduction and revenue enhancements.

Berk and DeMarzo (2017) examine in detail the synergies most often cited by acquirers to justify the takeover. A larger company can enjoy economies of scale and the savings from producing in greater volume (Berk & DeMarzo, 2017). The same can be seen in economies of scope, where larger firms have savings from combining marketing and distribution. With a vertical integration of the Acquirer and the Target, its distribution channels' coordination and control are the principal benefits. Another reason for a takeover is for a more efficient solution to purchase the talent and expertise as an already functioning unit in the Target firm. While Berk and DeMarzo (2017) also state monopoly gains as a reason to takeover the Target firm, in Norway, where The Norwegian Competition Authority conducts thorough investigations to ensure that the market is not monopolized[1], this could instead be translated to take a larger piece of the industry.
Larger ones are also acquiring many small firms because they can prove to have a missing ingredient necessary for the Target firms success (Brealey, Myers and Allen, 2017) - or the other way around. This is called having complementary resources. Here, a takeover might give opportunities neither firms would have otherwise.

Brealey, Myers, and Allen (2017) gives examples of occasions where the takeover achieves gains; "the Acquirer nevertheless loses because it pays too much for the Target firm. The buyer might overestimate the value of stale inventory or underestimate the costs of renovating old plants and equipment. It may also overlook the warranties on a defective product. The Acquirer needs to be particularly careful about environmental liabilities. If there is pollution from the Target firm's operations or toxic waste on its property, the cost of cleaning up will fall on the Acquirer". This is a literal wording from Brealey, Myers, and Allen (2017) with sustainability in mind, that can also be seen figuratively with other ways of bringing bad reputation.

As a positive increase in value can not always be expected after an acquisition, in other words, there are significant risks associated with making an acquisition. The takeover may considerably influence the combined firm's risk profile in terms of increased uncertainty about its future cash flows. Because prior research suggests that the

[1] "Derfor griper Konkurransetilsynet inn mot Schibsted og Nettbil." 11 nov.. 2020, https://shifter.no/a/196003. Opened 4 des.. 2020.

acquirer firm's shareholders mostly experience negative share price performance in the months following the announcement of the takeover (Agrawal & Jaffe, 2001; King, Dalton, Daily, & Covin, 2004), the shareholders expect the acquirer firm's managers to inform them about the acquisition risk level and its impact on the combined firm's risk profile. Also, Feix (2020) refers to studies showing that in the global merger and acquisition market, 50-70% of takeover deals fail.

2.1.2 Decreasing the Risk

Before committing to a takeover, managers usually conduct due diligence (Cullinan, Le Roux, & Weddigen, 2004; Perry & Herd, 2004; Rosenbloom, 2002). By reviewing the target firm's financial statements and anything else deemed material considered significant, they try to confirm the facts about the firm's ability to realize value from the acquisition. Because they identify and assess the risks associated with takeovers during due diligence, they gain access to private information about the takeovers risk level.

Also, Perry and Herd (2004) write that takeover failures can be attributed to poor synergy, bad timing, incompatible cultures, off-strategy decision-making, hubris, and greed. Making a deal work is one of the most challenging business tasks. As takeovers become increasingly complex, due diligence activities become more critical (Perry and Herd 2004). The Acquirer does not fail to do due diligence, they fail to do it well. Blaauw (2019) notes in particular that the buyer will, in any case, be concerned with reducing the transaction risk. The transaction risk is mainly about knowing what you are buying. It is in the nature of things that one will not completely eliminate the transaction risk. No one knows what the future will hold or what it will bring (Blaauw, 2019). Through adequate investigations, verification of the seller's information and statements, and proper protection mechanisms in the transaction agreement, the buyer will minimize the transaction risk. Blaauw (2019) takes a closer look at the buyer's aforementioned investigations, the seller's information, documentation, and statements regarding the target firm, which is called due diligence.

2.1.3 Due Diligence

According to Blaauw (2019), the common forms of due diligence are legal, financial, commercial, technical, ESG (Environmental, Social, and Governance), anti-corruption, and insurance. In recent times, where more and more companies are making money from or relying on technological systems in their operations, intellectual property, IT, and patent law are essential to check in the investigations before a takeover (Blaauw, 2019). Modern takeover processes are just now beginning to catch up to new technologies by including privacy and cybersecurity concerns as discrete issues within the traditional due diligence paradigm (Blaauw, 2019).

Feix (2020) states that “Due diligence intends a consistent, robust, and stress-tested proof-of-concept of the target company’s investment thesis. The due diligence process is highly complex and consists of multiple activities like site visits of the most important factories, sales outlets, and research & development centers. The assessment of the most critical documents in a virtual or physical data room as management presentations and discussions. The origin of due diligence lies in the information asymmetry between the buy and sell-side. The entrepreneur and the management team of the target company might know the company inside-out”.

The acquirer has in most cases, a minimal information level concerning the target company before the due diligence (Gole and Hilger, 2009). Due diligence also increases the probability that the buyer achieves the synergies that may motivate the acquisition (Aabø-Evensen, 2011).

Feix (2020) remarks on how the due diligence is intertwined with the Target firm's valuation and the purchase agreement. The indicative valuation is based on the assumed value drivers of the target company, and therefore, it might help prioritize due diligence tasks and deliverables. The due diligence outcomes, vice versa, are feedback into the update of the valuation. The most critical risks identified within the due diligence have to be either addressed in the purchase price or the purchasing contract, especially the deal structure or integration priorities (Feix, 2020).

Further, Feix (2020) states some core tasks of due diligence:

- "The investment thesis's verification is described in the indicative offer and the potential synergies, as those two components define the transaction rationale and purchase price limits.
- Gaining an in-depth understanding of the strategy, the business design, the culture Design, the competitive advantages, and the Target firm's value drivers.
- Besides, the evaluation and verification of the strategic fit between the target company and the acquirer, especially with respect to the Standalone Cultures Designs (SCDs) and Standalone Business Design (SBDs), is essential.
- The identification of essential strategic, legal, financial, operational, management, and cultural risks of a potential transaction. These have to be addressed either within the purchasing agreement or within the integration concept to avoid integration hurdles.
- Additionally, potential upsides and additional value drivers should be identified".

To fulfill these multiple tasks, the due diligence is built upon a couple of intertwined modules (Feix, 2020). Due diligence quality depends on a qualified due diligence team with precise tasks, responsibilities, communication, and structured sub-process.

A couple of due diligence success factors could be identified (Feix, 2020):

- "An early prioritization of questions and topics that should be addressed within the due diligence might support sustaining the focus and the due diligence's execution on the crucial value drivers of the target's business, the transaction rationale, and on the most critical risks. This also might avoid getting lost within highly complex and time-demanding due diligence processes.
- The due diligence project leadership or project house should establish clear roles and responsibilities for the due diligence teams. Besides, communication principles, on the one side between the due diligence leadership team and the different due diligence modules, and on the other side between the IPH due diligence leadership team and the top management, should be established. The latter might be essential, as within due diligence processes often fast management decisions are requested.
- In an E2E view, the Transaction Management has also to safeguard that the due diligence outcomes are fed into the update of the valuation and Synergy Management. The latter is significant for the proof of the likelihood and volume of synergies.

- The due diligence's identified risks have to be addressed in the purchase agreement, the transaction structure, and in the draft for the Integration Management.
- Especially for serial acquirers, the step-by-step build-up of due diligence capabilities and tools to foster learning effects and quality improvements for future acquisition processes is recommended".

2.1.4 Tech Due Diligence

"Anyone who fails to undertake a due diligence assessment, including a competent analysis of the underlying technology, may unsuspectingly invest in a superficially attractive but ultimately impossible enterprise" (Goforth, 2001). Goforth says, "similarly, a company that fails to acknowledge and respond to the risks inherent in new and developing technologies may be unable to attract needed investments or may find itself exposed to potential liability for claims made in connection with securities' issuance. Investment professionals may offer inappropriate advice or fail to give adequate warnings if the risks are not fully appreciated or articulated". The risks will be exposed only if an assessment of the technology is included as a fundamental and integral part of due diligence in the investment process. In order to fully appreciate these needs, it is vital to re-evaluate the meaning of specific essential terms (Goforth, 2001).

Goforth (2001) suggests that technology assessments should be integrated with conventional due diligence, providing a new focus for investment opportunities that are primarily technology-based and/or technology-driven. "For technology assessments to augment conventional due diligence, an intimate knowledge of the state-of-the-art in the relevant technology and technology trends, research and development management, and management technology is required" (Goforth, 2001). Goforth says that a high degree of research and scientific sophistication and a well-developed analytical methodology to evaluate the relative potential risks and rewards of the acquisition or investment in technology-based enterprises is necessary.

A successful IT due diligence is one of the most rewarding projects to be undertaken (Gleich et al., 2018). IT can, does, and should play a significant factor in making or breaking a takeover deal. The benefits of a well-executed IT due diligence will show immediately in a well defined and realistic view on potential synergies and IT post-merger integration evaluation. These are the factors that will primarily assist in evaluating a possible offer for the examined Target firm. Gleich states that it is important to carefully plan the transition, as it can be a special challenge when two different companies and IT cultures merge.

The IT due diligence should look at the Target firms and the Acquirers from several viewpoints (Gleich et al., 2018). Among the strategic fit of customers, markets, products and, so on, the potential new customers and markets for existing products, and the synergies resulting from overlapping business models.

Especially during the due diligence phase, operational experts from different divisions (finance, IT, HR) are expected to analyze large amounts of information and recommend courses of action. These persons are not usually a part of the due diligence process, and thus they need to be prepared for these special requirements during this time (Gleich et al., 2018).

"70% of merged companies combine information systems operations immediately after the merger transaction takes place, whilst up to 90% eventually combine information systems operations into a single data centre, usually within a year" (Sherer, Hoffman & Ortiz, 2015). They say that IT is likely to have a reactive role. IT must be integrated to consolidate other operations in the companies. For each of these activities, activities during merging IT systems are haphazard, as "acquisition-related activities—at least for most internal (and many external) parties—are by their nature non-routine processes that each require a tailored, expert approach".

2.1.4.1 Technology debt

"Technical debt is a metaphor for delayed software maintenance tasks" (Guo, Spinola, & Seaman, 2014). "Incurring technical debt may bring short-term benefits to a project, but such benefits are often achieved at the cost of extra work in future, analogous to paying interest on the debt. Currently technical debt is managed implicitly, if at all" Thinking about technical debt, it is usual to think of structural issues: spaghetti code, and leaky abstractions (Counsell, Antoniol, & Laplante, 2017). But in practice, there's a far more fearsome adversary: data.
Guo, Spinola, & Seaman (2014) states that technical debt management's impact on software projects is in particular, that there is a significant start-up cost when beginning to track and monitor technical debt, but the cost of ongoing management soon declines to very reasonable levels.

2.1.5 Cybersecurity due diligence

Cybersecurity concerns are only occasionally mentioned among many potential considerations within acquisitions (Sherer, Hoffman & Ortiz, 2015). This shows in the few findings on research articles related to cybersecurity, due diligence, and merger and acquisition. One of the articles that appeared is an article from the International Financial Law Review by K. Lai in 2019. This is closer to an opinion article that uses interviews with business leaders to build up the opinion. This shows that this angle of due diligence is beginning to receive attention. She writes that data privacy and cybersecurity have become increasingly crucial in technology takeover deals (Lai, 2019). Technology acquisition deals require a different due diligence process to traditional acquisition, especially for data privacy issues. Dealmakers must be hyper-aware of limiting data access to avoid snares in complex technology takeovers.

With the increasing risk of cybersecurity and strengthening personal information protection by relevant authorities, the importance placed on due diligence on personal information protection is rising (Mok, 2020).

Shonka and Rotert (2020) compare a takeover process with a poker game. The players have only limited opportunities to improve their hands before the betting ends. And when one company acquires another, the acquirer bets on the acquired entity's privacy and security practices. Shonka and Rotert (2020) continue to use the terms of poker games and say assessing risks is difficult because often, the acquiring company has little opportunity to evaluate the cards it does not see. It lacks visibility into the target's cybersecurity protocols and practices. The acquiring company may be forced to gamble with the cards it has been dealt, and the resulting losses can be significant (Shonka & Rotert, 2020).

In an article in Wall Street Journal Pro. Cyber Security, Nash and Minaya (2018) write about how Verizon Communications Inc. last year renegotiated an acquisition proposal with Yahoo Inc.'s board after details emerged about massive hacking incidents. Verizon would ultimately learn all three billion Yahoo accounts were hit. As a result, Verizon lowered its proposed purchase price by $350 million to $4.48 billion.

The company did studies to assess potential reputational harm and future risks, said Craig Silliman, Verizon's general counsel, speaking at a Wall Street Journal conference the year in front (Nash & Minaya, 2018). "We said, 'We feel like we have enough clarity that we can put parameters around the risk here and negotiate a deal that effectively compensates us for the risk.'"

In general, public scrutiny around acquisitions has increased for all companies involved in deals (Welgan, 2016). "Senior leadership, including the board of directors, must ensure that cybersecurity due diligence is conducted as faithfully as any other diligence area" (Welgan, 2016). New York Stock Exchange Governance Services survey from 2016 revealed that three-quarters of respondents said that a high-profile data breach at an acquisition target would have serious implications for a pending acquisition. "Moreover, more than half said that a high-profile cyber breach would diminish an acquisition target's value. While this is not the first time that cybersecurity issues have negatively affected stock prices, this may be the first case where cybersecurity disclosures—responsible or otherwise—were tactically used to affect interim company value and potentially derail an acquisition deal" (Welgan, 2016).

There are many considerations to take into account to avoid complicating acquisition plans (Welgan, 2016). The following are the top five:

1. "Are there any indications that the acquisition is currently breached or has previously been breached?
2. What is the acquisition's overall cybersecurity maturity? Cybersecurity equals cybermaturity. Be wary of acquisitions that have lackluster cybersecurity policies, procedures, reporting structure and training.
3. Has the organization conducted its own cybersecurity audit? When? By whom? What were the results?
4. What types of devices, systems and data does the acquisition have that may be at risk?
5. How are cybersecurity due diligence efforts being documented?"

Whether a refined duty of cyber diligence would cure or inflame the ills of cyberspace is still unclear (Jensen & Watts, 2017). "We are in the early days of cyber due diligence and, frankly, of the relationship between international law and cyberspace".

"70% of merged companies combine information systems operations immediately after the merger transaction takes place, whilst up to 90% eventually combine information systems operations into a single data centre, usually within a year" (Sherer, Hoffman & Ortiz, 2015). IT is likely to have a reactive role, in that it must be integrated to consolidate other operations. Finally, for each of these activities, ad hoc information systems merging activities are even more haphazard, as acquisition-related activities—at least for most internal (and many external) parties—are by their nature non-routine processes that each require a tailored, expert approach.

Cybersecurity concerns are only occasionally mentioned among many potential considerations within acquisitions (Sherer, Hoffman & Ortiz, 2015).

2.2 Cybersecurity Management

Cybersecurity is a term that has been used extensively in recent years. In the early phase of information technology, it was common to define and establish ICT Security and IT Security. Gradually Data Security and Information Security were used as terms. In recent years, Cyber Security and Digital Security have been used in both research and in businesses. The content and definition are mainly the same. Cybersecurity is "the preservation of confidentiality, integrity, and availability of information. Confidentiality, the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. Integrity, the property of accuracy and completeness and availability, the property of being accessible and usable on demand by an authorized entity" (ISO/IEC 27000:2018, 2018; ITGovernance, 2019)

In the report, I choose to use the term "cybersecurity".

2.2.1 Definition of Cybersecurity

As a result of a literature review done by Craigen, Diakun-Thibault, and Purse (2014), they selected nine definitions of the term cybersecurity that seemed to provide the material perspectives of cybersecurity:

Definition	**Reference**
Cybersecurity consists primarily of defensive methods used to detect and thwart would-be intruders.	Kemmerer, 2003
Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and malicious damage or disruption.	Lewis, 2006
Cybersecurity involves reducing the risk of a malicious attack to software, computers, and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on.	Amoroso, 2006
Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets.	ITU, 2009
The ability to protect or defend the use of cyberspace from cyber-attacks.	CNSS, 2010
The body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs, and data from attack, damage, or unauthorized access to ensure confidentiality, integrity, and availability.	Public Safety Canada, 2014
The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets, and critical infrastructure	Canongia & Mandarino, 2014
The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.	Oxford University Press, 2014
The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.	DHS, 2014

Table 2.1: Definitions of cybersecurity found in a literature review by Craigen, Diakun-Thibault, and Purse (2014)

There (Garfinkel, 2012) is no obvious solution to the problem of cybersecurity. "While depending on our computers, we seem incapable of making or operating them in a trustworthy manner. Much is known about how to build secure systems, but few of the people building and deploying systems today are versed in the literature or the techniques. Society should be designing to survive the failure of our machines, but it is more cost effective to create systems without redundancy or resiliency".

Reducing our cyber risk requires progress on both technical and political fronts. But despite the newfound attention that cybersecurity increasingly commands, our systems seem to be growing more vulnerable every year (Garfinkel 2012).

2.2.2 Security Incidents

Many factors decide what a security incident is, and many different definitions can be found (Ponemon 2018; ITRC & Cyberscout. 2017; Cate 2008; Rouse and Wigmore 2017). For this thesis, I have chosen to use the following definition:
"A security incident is an event that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed" (Rouse and Wigmore 2017).

For years, obtaining an overview of all identified security incidents has proven challenging. Companies still cannot confidently say that they have a total overview of all incidents they have experienced. There is no guarantee that information regarding the incident is made publicly available in many cases where incidents are identified. According to a report by the Identity Theft Resources Center in the United States alone, a total of 1579 data incidents were registered (ITRC & Cyberscout. 2017). The actual total is still unknown. The report shows that the number of incidents reported has increased by 46% compared to 2016. This development will probably continue, and even if all of the incidents are not registered, the number of incidents will most likely increase exponentially (Juchems 2018).

Since companies have no standardized requirements to disclose their security incidents, a realistic global total amount might not be obtainable. Finding reliable sources for information regarding incidents for a thesis such as this is therefore difficult. With that said, the increased attention, and most likely the introduction of regulatory requirements to report incidents such as the California Security Breach Information Act and the General Data Protection Regulation (GDPR), has resulted in more incidents being announced either by the affected companies, or the media.

As Garfinkel (2012) explains there is no obvious solution to the problem of cybersecurity. While we depend on our computers, we seem incapable of making or operating them in a trustworthy manner. Much is known about building secure systems, but few of the people building and deploying systems today are versed in the literature or the techniques. We should be designing society to survive our machines' failure, but it is more cost-effective to create systems without re-redundancy or resiliency.

"Reducing our cyber risk requires progress on both technical and political fronts" . But despite the newfound attention that cybersecurity increasingly commands, our systems seem to be growing more vulnerable every year" (Garfinkel, 2012).

2.2.3 Cost of Security Incidents

One of the more difficult challenges in cybersecurity is deducting quantifiable data. The lack of historical data makes it even harder to estimate what economic effects a security-related incident might have. While calculating the loss of a security incident is challenging in itself, it proves to be even more complicated when only about a quarter of the actual incidents that occur are reported. This leads to even more significant uncertainty as most historical data and research are most likely not of a realistic representation.

"The cost of system breach is often difficult to quantify. There are direct and enduring costs of information breach. As such, it has implications that impact the downtime for the ICT-systems during a data breach and loss of customers, trust, loyalty, and brand equity, all of great concern to marketing managers" (Choong et al, 2017). The results of the study of Choong, Hutton, Richardson, and Rinaldo (2017) indicate that the market punishes the firm with a small but significant negative abnormal return on the announcement of the breach, and this trend persists. This result, together with the indirect or enduring costs related to brand erosion, provides a good justification to senior executives for protecting the integrity of information, and by so doing, protecting the equity of the brand.

"Cybersecurity is moving up the agenda for institutional investors and their financial managers as a responsible investment consideration, as several high-profile attacks and breaches bring the issue to the front of investors' minds" (Baker, 2017). Coller Capital's latest Global Private Equity Barometer (2017) found that 45% of limited partners will require their general partners to do cybersecurity risk assessments for their portfolio companies within three to five years.

IBM Security's (Ponemon Institute, 2019) annual report, research by the Ponemon Institute, claims that the average cost of a breach is now $3.92m. Ponemon's research over the years shows a steady rise in the breaches' cost – an increase of 12% over the past five years. Having an incident response team in place and extensive use of encryption are the most effective ways of cushioning the impact of a breach, with an average reduction of $360,000 for each. Having undertaken extensive tests of your incident response plan is also very helpful. Organisations with fully deployed security automation technologies experienced around half the cost of a breach ($2.65m average) compared to those that did not have these technologies ($5.16m).

Sponsored by IBM Security and conducted by the Ponemon Institute (2019), the annual Cost of a Data Breach Report is based on in-depth interviews with more than 500 companies worldwide that suffered a breach over the past year. The analysis takes into account hundreds of cost factors including legal, regulatory and technical activities to loss of brand equity, customers, and employee productivity. Some of the top findings from this year's report include:

Finding	Meaning
Malicious Breaches – Most Common, Most Expensive	Over 50% of data breaches in the study resulted from malicious cyberattacks and cost companies $1 million more on average than those originating from accidental causes.
"Mega Breaches" Lead to Mega Losses	While less common, breaches of more than 1 million records cost companies a projected $42 million in losses; and those of 50 million records are projected to cost companies $388 million.
Practice Makes Perfect	Companies with an incident response team that also extensively tested their incident response plan experienced $1.23 million less in data breach costs on average than those that had neither measure in place.
U.S. Breaches Cost Double	The average cost of a breach in the U.S. is $8.19 million, more than double the worldwide average.
Healthcare Breaches Cost the Most	For the 9th year in a row, healthcare organizations had the highest cost of a breach – nearly $6.5 million on average (over 60% more than other industries in the study).

Table 2.2: Findings in IBM Security's (Ponemon Institute, 2019) annual report

Acruri, Brogi, and Gandolfi (2014) found that cyberattacks' announcements affect the stock market returns. In particular, we found evidence of an overall negative stock market reaction to public announcements of cybersecurity breaches. Understanding the true impact of cyberattacks on the stock market returns is crucial to decide investments in cybersecurity activities. The issue is made particularly actual by the proliferation of information technology and the internet. Acruri, Brogi, and Gandolfi (2014) also showed that stock market reactions differ according to firms' economic sector. Above all, some firms need to equip themselves with control systems that monitor exposure to cyber risk to reduce financial and reputational losses (Acruri, Brogi, and Gandolfi, 2014).

In his master thesis Shaikh (2018) does a quantitative incident study analysis on the effect of cybersecurity incidents for the stock price value. The results show that announcing a breach can have an effect on the value of the company in certain situations. There is a strong correlation between announcing an incident and the value the affected company has on the stock market. An interesting takeaway is that rather than focusing on how an industry experiences the effect of an incident, it is the type of information affected that shows the strongest effect of announcing an incident.

A study of Hinz, Nofer, Schiereck, and Trilig (2015) examined the reactions of the capital market to a security incident at consumer electronics companies, which have implications for the economically optimal level of investment in cybersecurity. Hinz, Nofer, Schiereck, and Trilig (2015) analyzed the impact of data theft on share prices and systematic risk. Their results illustrate that the disclosure of a security incident leads to a significant decline in the affected company's share price. Negative returns on the stock price can be observed also over a 10-day window following the announcement. It is also

done studies by Garg et al. (2003), Cavusoglu et al. (2004), and Campbell (2003) that have given the same results of negative stock market reactions to security incidents.

2.3 Framework - Capability Maturity Model Integration

The Capability Maturity Model Integration (CMMI) (the Software Engineering Institute (SEI), 2008; Ayyagari, 2019) is a process improvement framework developed more than 20 years ago and governed by the Software Engineering Institute (SEI) at Carnegie Mellon University (USA). CMMI is sponsored by the U.S. government (especially the U.S. Department of Defense) and is in use by organization's of all sizes worldwide. It has helped to streamline costs, reduce rework and defect rates, and improve timelines and quality.

By itself, CMMI is a process improvement framework developed to address a broad range of application environments. There are three different models based on the CMMI framework:

- CMMI for Development (CMMI-DEV), a process model for process management and improvement in software development organizations

- CMMI for Acquisition (CMMI-ACQ), a model for organizations that have to initiate and manage the acquisition of products and services

- CMMI for Services (CMMI-SVC), a process model for organizations to help them to deploy and manage services

Ayyagari (2019) writes that the Capability Maturity Model Integration follows a set of stages known as the CMMI levels from one to five that determine an organization maturity level. Therefore, as the organization raises its maturity level to a higher level, it increases productivity, Return on Investments, and resource utilization.

The CMMI-ACQ applies CMMI's best practices in an acquiring organization. The best practices in the model focus on activities for initiating and managing the acquisition of products or services to meet customers and end users' requirements.

The CMMI for Acquisition is designed for the purchase of products or services. Nevertheless, I have decided to use this framework in the context of acquiring an entire company. There are some differences between a product or service and an entire company, but the principle of acquisition, and quality assurance and maturity are generally the same.

The most common view of the CMMI is a series of stages of maturity from one to five. The five levels from one to five embodies an organizational plateau of the overall capability of the organization. Each level has a predefined set of assigned processes for cohesive implementations and results.

The different levels in the CMMI is:

- Level 1 Initial
- Level 2 Managed
- Level 3 Defined
- Lever 4 Quantitatively Managed
- Level 5 Optimizing

At level one, the organization practices are ad hoc; therefore, there are no PAs at this level. Level two (managed), have practices of project management and product support practices that convert requirements to accepted products. Level three (defined), has an organized process as described in standards and the organization measures. Level four (quantitatively managed), has a continually improved process through iterative and incremental technologies. The last, level five (optimizing), establishes the finetuning of organizational processes and practices. An organization strives to target the highest level based on current constraints and environmental factors.

In a dynamic and rapidly changing world, that constant technological development creates, organizations need to have dynamic capabilities (Ayyagari, 2019). Ayyagari (2019) connects, therefore, the CMMI to Teece's (2018) concept of dynamic capabilities ensures business corporate agility. The model consists of three main components: a sense that identifies opportunities and threats of technology, seize opportunities using resource and business models and transform apprehended opportunities by investing in new capabilities.

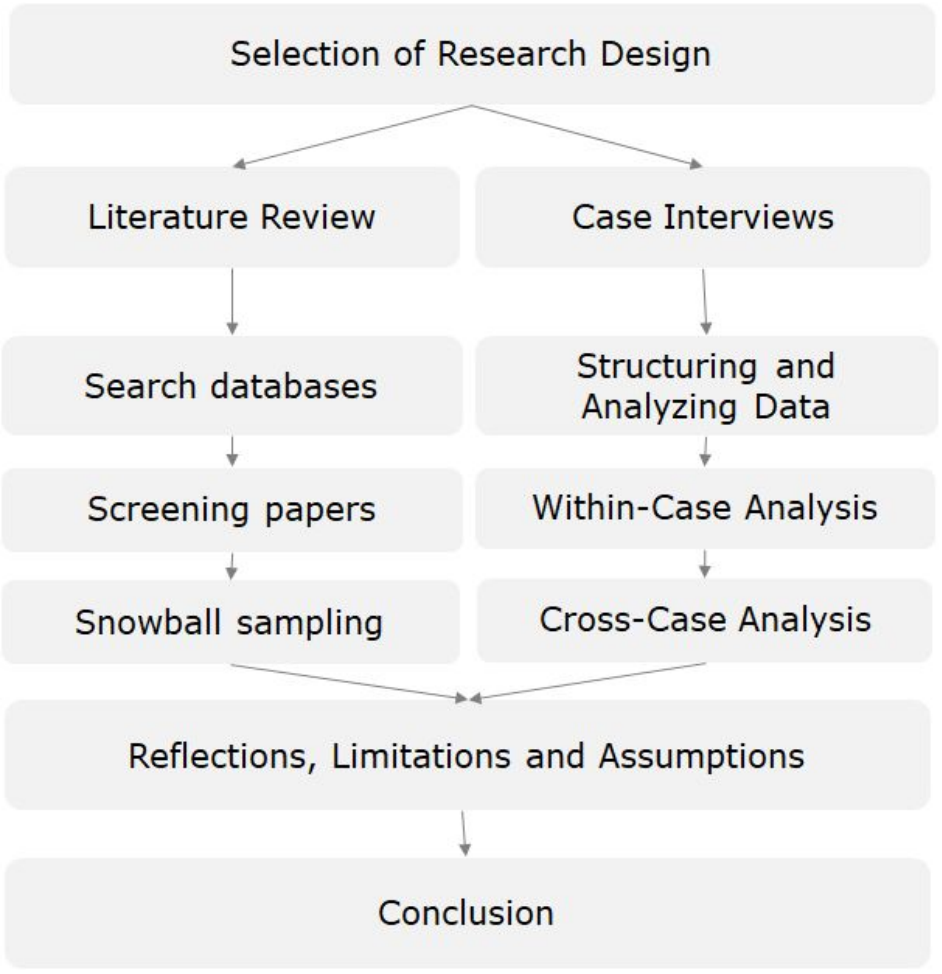
I have taken parts from CMMI-ACQ together with parts from Cyber Maturity Model Integration, and ended up with a "cybersecurity maturity acquisition integration model".

If a CMMI level five certified organization meets up with a lesser certified one, this can create tensions and problems regarding approaches for projects (Gleich et al., 2018). One of the major challenges, in this instance, will be to quickly transform the part of the organization lacking the relevant certification and bring it up to par with the other one. An additional cost to be considered here is that many personnel may need to be recertified.

Chapter 3 - Method

In this chapter, I will present the method used for the study. The presentation includes describing the research design, the selection process of the cases, primary and secondary sources of data collection, the methodology of data analysis, and a reflection on the chosen method and its limitations.

To answer the thesis' research question, I have chosen a qualitative method to collect data. The qualitative, semi-structured interviews are the primary source for data collection, together with the literature review. As a secondary source, I have used the case firms' annual reports, websites, news articles, and industry reports. The secondary source is to fill potential gaps in knowledge or gaps in previous research to have a broader foundation on which to build the interviews and fill in areas where the interviewees cannot answer in full. The secondary data sources are used only as a supplement and to collect information for structuring the interviews.



3.1 Selection of Research Design

When I first started working towards the master's thesis in the autumn of 2018, I began looking at whether it was possible to combine the fields of finance, entrepreneurship, and cybersecurity. I wanted to have a broad purpose for the work of the thesis, and talked to professionals in different industries and subjects. I got a wide variety of different interesting topics depending on the industry and the background of the person I spoke to. The most fundamental differences were between the professionals from finance and from cybersecurity. The professionals from private equity said, among other things, that looking at cybersecurity in connection with, for example, investments were not engaging as this was not usually looked at. From the cybersecurity environment, it was said that this was an interesting angle. They thought I would get interesting answers that were not looked at to any great extent . In other words, they described the same topic but interpreted the interest in the response in different ways. For me, these answers motivated me to continue the search further. I went on to look at how cybersecurity can affect the decision to invest in a company. That is, whether an investor examines the company's cybersecurity in advance of a potential investment. In connection with this issue, I looked up literature related to decision theory on investments. I also spoke with several in-house consultants in cybersecurity and consultants who work with a new and more specific technology due diligence. Again, I received very different answers connected to whether the company had a financial interest in its opinion. A consultancy company that works with technology due diligence will state it is crucial to examine its technology to be bought up or invested in. A company that works with financial due diligence will, of course, believe that technology due diligence is not as necessary. Here I did further literature searches also on mergers and acquisitions. The new literature search gave me some more research findings related to due diligence in advance of an acquisition. Thus, I decided to significantly delimit the thesis' topic by looking at how cybersecurity is examined in advance of an acquisition. To get in touch with decision-makers and the right people, I also decided to limit the task of looking at companies in Norway as they are more reachable for me to get in touch with. Then I started the literature search used in this thesis.

With my background in cybersecurity studies and entrepreneurship studies and an active role in Norway's entrepreneurship environment since 2016, I had both the network to get answers to these questions and the prior knowledge to understand them and put them in context.

There are two main research methods to adopt when performing social research - quantitative and qualitative (Flick, 2015). While quantitative research methods weigh more extensive data collections in a standardized structured interview, qualitative research methods provide more in-depth insights beyond these standardized interviews. A qualitative research method is favorable when the thesis wishes to gain deeper insights into the research questions. Since the purpose is concerned with "how" something works or takes place, a qualitative method was the most suitable choice for

this study (Yin, 2014). The method is preferred above quantitative studies when the researcher aims to gather and analyze experiences that are difficult to quantify or measure (Dalland, 2012). The thesis's purpose, which is to investigate how the Bidder considers potential Target firms cybersecurity. A qualitative study will give both thoughts and insights of actors working in this field to fulfill this purpose. Furthermore, qualitative research is suited for a small number of cases, many different sets of variables, and wants to connect the research with existing theory (Yin, 2017).

The Abductive Research Strategy is another essential and promising type of qualitative research methodology, developed by some social scientists and elaborated by Blaikie (2010). As expounded by Blaikie (2010), the idea of abduction refers to the process of generating social scientific accounts from social actors' accounts. Technical concepts and theories are derived from lay concepts and interpretations of social life. Hence, the aim of the abductive Research Strategy is the construction of theories that are grounded in everyday activities, in the language and meanings of social actors. In order to develop this research strategy, Blaikie (2010) has drawn a great deal on the work. Attention is given to the meanings and interpretations, the motives and intentions, which people use in their daily lives, including the meanings and interpretations people give to their actions, other people's actions, social situations, and natural and humanly created objects. This is because the social world is interpreted and experienced by social actors from the 'inside'. People use largely tacit, mutual knowledge, symbolic meanings, motives, and rules, which is assumed to provide direction to their actions – to do what they do in daily life (Blaikie, 2010).

The study is formed as an exploratory study as it seeks to ask questions and assess a specific phenomenon in a new light (Yin, 2014), which fits the thesis's purpose. Exploratory studies are useful when researchers lack a complete understanding of an area of research and the authors need new insights (Yin, 2014), in this case, information asymmetries between Bidder and the Target firm. Exploratory studies have the goal of explaining the relationships between the variables in a situation and are especially fruitful in areas where the lack of existing research is scarce. As the authors seek to explore the relatively unexplored area of how information asymmetries between private investors and the venture capital firm can be managed by trust in a deal-by-deal structure, an exploratory study is appropriate.

This thesis's study is carried out as a multiple-case study, where three different group companies with technology and data as some of the main focus areas for operation and income, which also buys other companies for growth, have been interviewed. These will further be referred to as "cases." Case studies allow for holistic and meaningful characteristics of real-life incidents as it enables us to understand complex situations (Yin, 2017).

I chose to conduct semi-structured interviews as it fits well with the purpose of the thesis and allows the authors to expand their understanding of the research subject (Dubois & Gadde, 2002). The semi-structured interview allowed me to use probe questions when they saw it necessary for the interviewees to further explain or widen their answer (Saunders et al. 2012). This facilitates the possibility to discover new topics that have not been covered by existing theoretical frameworks, which is a central element for an abductive research approach (Dubois & Gadde, 2002). Debois and Gadde (2002) described that a high number of cases is not systematically the same as getting better results. In order to know that one has obtained systematic results, a lot of

interview objects are needed to be able to put the results in a system and compare them. For a qualitative study, going in depth with a few could give a similarly good result. Especially in this study, it will be natural to get some answers from a few companies and get to know more about each of those companies and their working methods in order to gain some foothold for further studies.

Ontology is about how one looks at the world. This is about what reality looks like and how to understand the world through scientific concepts, models, and theories. Furthermore, we have epistemology, which is the doctrine of knowledge. Epistemology is about acquiring knowledge and what practices and routines are used to gain understanding (Jacobsen, 2005).

3.2. Data collection

The information obtained and used in this thesis is obtained mainly from two sources. The three sources are the literature study, and the multiple case study interviews. I will present the data source for the study, how the sources are used, and why they are used in this subchapter.

3.2.1 Literature review

A literature acquisition is made to create the thesis's contextual background, and several studies and articles are reviewed. The findings are presented in chapter 2 about the literature review. This, together with the case study, forms the empirical data foundation for the thesis.

With the literature review, a study of industry reports of the industry's ongoing situation forms the thesis's data foundation.

Publisher	**Name of Industry Report**
Accenture	
Atea	The Financial Report 2014, 2015, 2016, 2017, 2018, 2019
CGI & Oxford Economics	
Ponemon Institute	IBM: Cost of a Data Breach Report 2019
Storebrand	The Financial Report 2014, 2015, 2016, 2017, 2018, 2019
Visma	The Financial Report 2014, 2015, 2016, 2017, 2018, 2019
World Economic Forum	The Global Risks Report 2007 - 2020

Table 3.1: List of reports used in the thesis

In this master's thesis, I have done a literature study that looks at the acquisition process and due diligence, and cybersecurity and how security breaches affect companies' finances. The literature of the study builds on the project thesis, submitted as a separate thesis for the project report written in TIØ4530 as part of the master's program at NTNU School of Entrepreneurship.

The sources used in the literature review is limited to the databases accessible through The Norwegian University of Science and Technology (NTNU). I have searched for relevant articles, books, and studies at Oria, Scopus, Emerald Insight, and Google Scholar.

3.2.1.1 Keywords and search strings applied for the literature findings

The following keywords are used in the search for relevant literature. In table 3.2. the keywords are listed in alphabetical order.

Keywords
Acquire
Acquire Norway
Acquire technology
Acquisition
Asymmetric Information M&A
Cybersecurity
Cybersecurity breach
Cybersecurity breach Cost
Cybersecurity due diligence
Data breach
Data breach Cost
Data Security
Due diligence
Due diligence cyber
Information Security
Information Security Breach
Information Security Breach Cost
M&A
Merger and Acquisition
Oppkjøp
Privacy Breach
Security Breach
Security Breach Cost
Tech due diligence

Table 3.2: Keywords and search strings applied for the literature findings

I also included unpublished and non-peer-reviewed articles for that search string as these kinds of papers can be just as crucial as other articles (Galvan, 2017).

In total, I have collected and read approximately 250 articles from the search strings. Not all the papers were relevant to the topic and the research question.
In total, I found 57 articles, which are used in the literature review.

The literature review findings are distributed as follows on the various topics that have been reviewed in the literature study.

Subject	**Number of Articles and Books**
Merger and Acquisition	1
The Takeover Process	8
Decreasing the Risk	4
Due diligence	4
Technology due diligence	4
Cybersecurity due diligence	7
Cybersecurity	13
Security Incidents	6
The cost of security incidents	10
Total of Articles and Books	**57**

Table 3.3: Number of Articles and Books

3.2.2 Multiple Case Study Interviews

I used semi-structured interviews using an interview guide. I structured the interviews in categories with some questions under each category. The categories' order did not play any role and was mainly determined according to how the conversation with the interviewee flowed. The semi-structured interview guide made each interview quite different from each other, but I made sure that all the categories and questions were covered. In the interviews, follow-up questions were also asked that were not in the interview guide when their answers were not anticipated.

Due to the Corona situation, all of the interviews were held by video conference systems. I conducted all interviews in October and November 2020. The primary data gathered for this thesis is from these in-depth interviews.

As mentioned in chapter 3.1, a qualitative study has been conducted with semi-structured interviews. It will be presented here which criteria have been used to select the interview objects used for the data collection. There are also some criteria

based on what type of companies this should not be, especially in the health industry, as it might be more extensive with cybersecurity.

At the beginning of the process of writing the thesis, an assessment was conducted on which companies might be relevant to interview for data collection. In this context, a list was written of criteria these companies had to fall under. The criteria were:

Criteria	**Justification**
Norwegian company with headquarters in Norway	Easier getting connected with. Also, for scoping the thesis to the Norwegian business market.
Made acquisitions in the period 2015 to 2020	This is the period from not knowing about GDPR to GDPR came into force
Has an employee in the position CISO and an associated department with professionals in cybersecurity	To be sure they have a basic understanding of the importance of cybersecurity and to know they have competence internally.
Having technology as a "critical" part of business operations. This means that normal operation will not be possible without technological tools, that the sources of income come from the sale of technological tools, either software or hardware.	Gives a better understanding of cybersecurity. They have a greater risk of major damage in a security incident, which should make them more cautious about stepping into new risks. In addition, this provides experience with the risks and they know what they are looking for in similar companies.
Public financial reports	To find the information they communicate to stakeholders and potential and existing investors.

Table 3.4: Criterias for case firms

Among the findings in this search, ten firms were selected who were contacted through email, messages via LinkedIn or telephone or by telephone call where it was stated that it was desired to conduct an interview with a relevant person from the company for a master's thesis with current research questions. Of these, three positive responses were received, stating that they both had time to do the interview and to contribute.

In addition, there were some negative answers where there was either a lack of time and resources or that they did not consider themselves relevant in terms of the research question and the focus of the thesis. Among these was a press release from one of the companies, which was asked two days after receiving an answer that they did not have the time and resources to contribute to master's theses now that they had acquired another company that week. Some of these have responded to messages quoted in the thesis but do not satisfy the requirements to be counted as an interviewee.

Person	Company	Acquired the last three years	CISO + Cybersecurity division	Tech in business operation	Public Financial Reports
Max Graff	Visma	Yes	Yes	Yes	Yes
Espen Johansen	Visma	Yes	Yes	Yes	Yes
Tore Lind	Storebrand	Yes	Yes	Yes	Yes
Steinar Sønsteby	Atea	Yes	Yes	Yes	Yes

Table 3.5: Case firms meeting criterias

The interviews that were conducted were conducted in October and November 2020. An interview guide was prepared in advance, which contained topics and questions that were to be reviewed during the interview. This was done to ensure that all the interviews covered the same categories and issues and the opportunity to answer some of the same questions. However, the interviews were not held in a particular order as it was preferably arranged for the interviewees to speak freely according to their own thoughts along the way as it came naturally. If a topic nevertheless did not naturally emerge, follow-up questions were asked along the way.
All of the interviews were conducted via video. I chose video for the interviews mainly due to the restrictions associated with the corona eruption in Oslo. It would have been desirable to be able to complete the interviews face to face. The interviews were recorded with the consent of the interviewees and then transcribed. This is on the recommendation of Yin (2017) to give the interviewer full focus on holding the interview, steer the conversation in the right direction, and be able to ask good follow-up questions.

Before the interviews, a general interview guide was developed with the knowledge of existing literature in mind. The gained insights were used as an inspiration for open questions to the semi-structured interview. The questions were sorted into different categories.

3.2.3 Other sources

Finally, it should be added that data collection has also been done from sources that are covered under the criteria but which have not been thoroughly interviewed, news articles, opinion articles, and the websites of the companies that have been interviewed. These are used to cover areas that the interviews or literature study do not cover or justify why literature studies have been done or questions to the interviewees.

3.3 Structuring and Analyzing the Data

The next step of my research process was to use the raw materials from the interviews to extract useful data that would be analyzed. After each interview, the interview record was listened to, and more detailed notes were taken. The transcription was done manually to ensure high quality and that all the interviewees' nuances from the interviews were considered.

NVivo was used to categorize and analyze the data into different categories, as suggested by Dubois and Gadde (2002). I used the newest NVivo version (11.3.2.) that was available for the students of NTNU. First, the transcripts, the detailed notes, and the recordings were imported to the software with the names of the firms as their titles. This way, the notes could be compared later. Using NVivo, I made codes based on the framework from Chapter 2 and structured and categorized the data. I started this coding separately on each interview and after that went through all the material and did the final coding together. Then nodes based on the theory were created. The nodes created for acquisitions and Cybersecurity also had subcategories. During the coding process, specific themes not theorized came up several times. One example is how GDPR (General Data Protection Regulation) affected the interviewee's thoughts in the process. Based on these themes, new nodes were created. When the transcripts were coded, each node displayed all the sentences categorized in that node.

The thesis takes an abductive research approach, which Dubois & Gadde (2002) referred to as "systematic combining."

3.3.1 Within-Case Analysis

The data was first sorted and coded by each case into the chosen categories, and then analyze what has been said and write it out into a more systematic text to analyze further. Further, the sorted data was coded into first-order codes, staying as close as possible to the empirical data to keep the respondents' perceptions detailed. Thematic categories were further subcategorized, where I examined and recorded patterns (Guest, 2012). Finally, the categories were also sorted into the matching mechanisms found in theory. This theory was used as a guide to code the material. However, the findings were not forced into themes and categories if the data set could not adequately justify it.

3.3.2 Cross-Case Analysis

After the within-case analysis, a cross-case analysis was conducted to inspect the cases from a holistic view. Eisenhardt (1989) states that cross-case analysis improves the chance of getting reliable data to build theories on and the possibility of discovering novel contributions. According to Yin (2015), the analyzed in-depth interviews' validity is increased by triangulating data. Therefore the data was analyzed in the context of data from the firm's annual reports.

The cross-case analysis is a research method that facilitates the comparison of commonalities and differences in the events, activities, and processes that are the units of analyses in case studies. The cross-case analysis is a research method that can mobilize knowledge from individual case studies. Engaging in cross-case analysis extends the investigator's expertise beyond the single case. It provokes the researcher's

imagination, prompts new questions, reveals new dimensions, produces alternatives, generates models, and constructs ideals and utopias (Stretton, 1969).

The cross-case analysis enables me to delineate the combination of factors that may have contributed to the case's outcomes. The cross-case analysis also seeks and explains why one case is different or the same as the others and makes sense of puzzling or unique findings. It can also explain the concepts, hypotheses, or theories discovered or constructed from the original case. Cross-case analysis enhances researchers' capacities to understand how relationships may exist among discrete cases, accumulate knowledge from the original case, refine and develop concepts (Ragin, 1997), and build or test theory (Eckstein, 2002).

Furthermore, cross-case analysis allows me to compare cases from one or more settings, communities, or groups. This provides opportunities to learn from different cases and gather critical evidence to modify the policy.

3.4 Reflection on the Method

The research methodology's limitations and weaknesses must all be considered as potential influential factors of this thesis' outcome. To reflect upon the quality of the research in this study, I use the concept of trustworthiness as presented by Guba and Lincoln (1989) and Erlandson et al. (1993) and discuss the thesis' credibility, transferability, dependability, and confirmability as cited in Halldórsson and Aastrup (2003).

Credibility is whether the thesis' reader has confidence that the findings of the study are correct. One of the techniques to increase credibility is to prolong the engagement of the interview respondent (Lincoln & Guba, 1985). This shorter interaction of just one interview can cause a lack of prolonged engagement. The reality of the respondents only exists in the minds of the respondents (Halldorsson & Aastrup, 2003). Therefore, a viable question is whether the data from the respondents is trustworthy. Collecting data from interviews after the end, the collaborations can lead to cognitive biases that can challenge the research's validity.

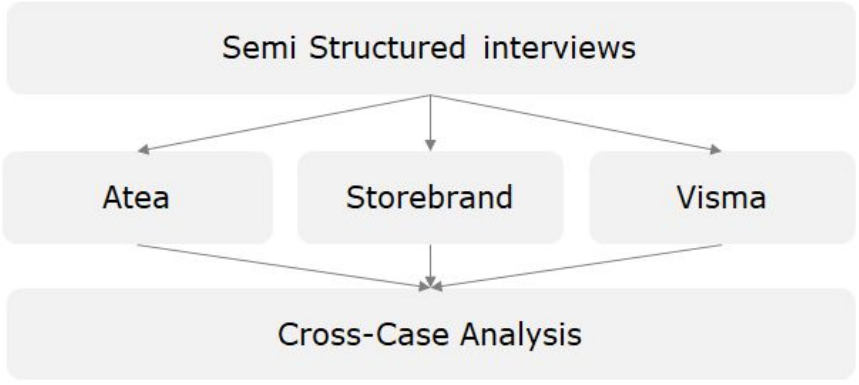
Transferability attempts to identify to which extent findings can be generalized or applied in other contexts or settings than the one studied. The transferability is, by nature, hard to estimate in qualitative research due to the way data is collected in different contexts over time (Erlandson et al., 1993). Nonetheless, the insights extracted from the data in one context can be relevant in other contexts. In such a case it is of essence that the person using the results in another setting understands the original context of findings (Erlandson et al., 1993).

Dependability concerns the stability of data over time (Lincoln & Guba, 1985). The dependability of research depends on showing that the findings are consistent and could be repeated if replicated. The dependability aspect of a research paper is concerned with whether the authors would reach the same conclusions if they could make the same observations twice (Lincoln & Guba, 1985).

Confirmability
"The extent to which the respondents shape the findings of a study and not researcher bias, motivation, or interest" (Lincoln & Guba, 1985). **Confirmability** is related to the objectiveness of the researchers conducting the study – whether the results of the study could be confirmed or developed by others (Halldorsson & Aastrup, 2003). Therefore it is important that the findings are solely based on the data itself, and not the opinions of the authors.

Chapter 4 - Findings and Analytics

This section presents the analysis of the data collected through semi-structured interviews and the qualitative method presented in chapter 3. I will present the interviews and cases one by one in alphabetic order. As the cases are introduced, they will also be analyzed and discussed. The case presentation is a summarized version of the transcribed interviews with some added information from the case firms' websites and their annual reports. In chapter 4.5, the cases are analyzed across cases together to see similarities and differences.



4.1 Atea

Atea is the market leader in IT infrastructure for businesses and public-sector organizations in Europe's Nordic and Baltic regions. Atea combines a breadth of competence in IT infrastructure with a local presence in each market they serve. They have approximately 7,000 employees located in 85 offices across seven countries. Atea offers a full range of hardware and software from the world's top technology companies. Atea has a range of international partners, like Apple, HP, Cisco, Citrix, Microsoft, and IBM. In addition to the partners, Atea also has close cooperation with approximately 70 companies. Atea has a team of specialist consultants with technical certifications and system integration skills to design, implement, and operate solutions for even the most complex IT requirements (Atea, n.d.).

Atea describes how corporate governance contributes to the creation of value and builds trust externally and internally. Atea states that decent corporate governance requires both satisfactory and efficient cooperation between the management and the Board of Directors, respect for the company's other stakeholders, and open and honest external communication. Atea also has established guidelines for internal control, which include routines for financial reporting, communication, authorization, risk management, ethics, and social responsibility. In order to ensure internal control and manage risk, the Group conducts comprehensive financial reporting and reconciliation on a monthly basis, on both a consolidated, segment, and subsidiary level. All financial reporting within the Group is in accordance with IFRS.

4.1.1 Relevance for the research

Atea is a company gradually built up by different kinds of mergers and acquisitions. Atea's parent company was founded in 1968 under the name Merkantildata, as a pioneer within the emerging market for information technology within Norway. The company became the largest IT infrastructure provider and related services in Norway and was listed on the Oslo Stock Exchange in 1985. The company's modern history dates to 2006, when Merkantildata (then called Ementor) merged with Top Nordic, the largest IT infrastructure provider in Denmark. The combined company then acquired Atea, the largest IT infrastructure provider in Sweden. The takeover was followed in 2007 by acquiring Sonex Group, the largest IT infrastructure provider in the Baltic region (Atea, n.d.).

The merged company took the name Atea in 2009. Atea then took the initiative to further consolidate the market by acquiring more than 50 companies, building additional market presence and scale advantages in its core geographies. Through acquisitions and organic growth, Atea has achieved an unrivaled position across the Nordic and Baltic regions, providing customers with a unique range of product competence and local market presence (Atea, n.d.).

4.1.2 The Interviewee

After a search of "Atea oppkjøp" the results gave several articles about Atea's acquisitions and Steinar Sønsteby's role in these takeovers. After I reached out, Steinar

said yea right away, and the qualitative semi-structured interview was conducted the day after.

Steinar Sønsteby is the CEO of Atea ASA (Atea, n.d.). Steinar Sønsteby joined Atea in 1997 and was managing director of Atea in Norway in 1997- 2000 and for Atea in Sweden in 2000 - 2002. Sønsteby was CEO of Atea Norway until 2012 when he became Executive Senior Vice President of Atea ASA. In 2014 Sønsteby was appointed CEO of Atea ASA. Before joining Atea, he was the CEO of Skrivervik Data AS.

4.1.3 Organizing the Acquisitions

Atea believes it is essential to use specialists in various subject areas. Atea mainly uses its own resources for the multiple reviews in a takeover. Sometimes, Atea does two reviews in the same subject area, one done by Atea's internal people and one that takes place with external resources. These two reviews are compared, and then they look at an overall result to assess whether the quality is sufficient. He mentions in particular two areas where external specialists are used. The first is for code review. Sometimes Atea also selects suppliers who are recognized for reassuring customers and other stakeholders. For the legal part of the due diligence, Atea always uses external suppliers.

4.1.4 The Takeover Process

Sønsteby describes two different forms of acquisitions. One variant is an opportunistic acquisition that happens once. Examples of this are the merger of Statoil and Hydro. When a new company is established in this way, a mix of the processes, organization, and technology is taken from both companies. Cybersecurity is critical in such situations and becomes more and more essential in a short amount of time. Another example was when Cisco bought Tandberg, where the technology assessment was absolutely decisive for the acquisition.

Atea normally makes the second form of acquisition, which is often called Series Acquisition. Acquisitions are part of the company's strategy, and there is a separate process that takes place each time. The new company will be part of Atea's infrastructure, and the IT part of the company will not be used in it further. Then a review of IT and cybersecurity is less critical. An example is an acquisition of a small consulting company with about 50 employees. Atea then considers mostly how the costs of the company can be stopped. They want to move the company as soon as possible over to the infrastructure in the parent company.

Atea has also acquired companies where Intellectual Property is being acquired. Atea does and has always done due diligence on the products. The source code is reviewed with regard to quality, and cybersecurity is an essential part of quality.

Previously, the company was valued based on value and turnover or intellectual property. Atea still looks at such values, but now also looks at the digital debt in the company. By this, Atea means how underinvested the company is within IT. The most important thing to look at is cybersecurity. If the company is hacked or has significant vulnerabilities, the company can be worth next to nothing. In such cases, IT and cybersecurity are a vital part of due diligence. If the Company's Software is a significant

part of the Company's value, Atea will perform two independent due diligence. One that is done by own people and one that happens with the use of external resources.

4.1.5 The Due Diligence Process

Atea does due diligence on the following aspects; Risk management, where cybersecurity is an important part, Legal, HR, Contract Law, Products, and Financial.

Since 2018, GDPR has been a completely new part of the acquisition process for Atea. Before, they did not spend time on the privacy requirements. GDPR changed the focus, as, for example, illegal collection of personal data has a retroactive effect. If the company does not comply with the GDPR and the way personal data is processed, this has a retroactive effect. If this is the case, it doesn't matter if Atea takes the data into its own company. Atea then assesses the quality of the system and the data contained in the system. The legality and basis for processing, as well as the data subjects' rights, are essential to gain status. These GDPR requirements are demanding to comply with and have received a significantly changed focus since 2018. GDPR compliance has been a primary internal task for Atea, and the internal methodology and structure of the work is also used in assessing the company's data.

Atea has reported from all due diligence assessments. All findings are then considered, and Tech due diligence and discoveries can also be decisive for whether the company is acquired. If Atea considers that the results are possible to live with, it impacts the price. The interviewee had examples of acquisitions being stopped due to tech-due diligence.

"Is it 'No-go' on Tech due diligence is it showstoppers regardless of price,"

Steinar Sønsteby, CEO Atea

It is not only when acquiring doing cybersecurity due diligence is essential. Atea has started the company AppExite. The company is an external company but fully owned by Atea. In such cases, requirements for cybersecurity are fundamental. In this company, external resources do annual due diligence. Also, tech due diligence helps to put the company's correct value.

For Atea's operations centers, independent source code reviews are also carried out, focusing on cybersecurity. This is important to secure the information for Atea's customers.

Taking over operations for other companies is reminiscent of acquisitions (outsourcing). Atea takes over tasks for essential parts of the IT infrastructure for customers. Even if it is not an acquisition, the risk associated with the IT part will be similar. Atea needs to know the quality of the systems and do due diligence on these. Serious security incidents for the customer will affect Atea's reputation.

Atea explains how they view the differences in acquiring a company where they will mainly have the employees and the customer portfolio and buy a company that develops its product and thus has intellectual property as part of its value. When they buy a company where they will have the employees and customer portfolios, there is IT infrastructure in the company they could do due diligence on, but since they will put it over to their own IT infrastructure and not use the one they already have, it is not some big point in doing technology due diligence. When they buy companies with intellectual property, such as software companies, they do, and here it is emphasized that they have always done this, due diligence where they look at the technology and go through all the source code. In such a review, cybersecurity is a big part of it. Here, too, cybersecurity has become more critical in recent years, but not as much of a difference. It has always been essential.

Atea does due diligence itself, as well as an external team also does due diligence. Then they can compare the results. This creates discussions, which opens up for better valuation of the company that is being assessed.

4.1.6 Cybersecurity

With such acquisitions, there has been a revolution recently in terms of the focus on cybersecurity. The interviewee knows some businesses in the USA, personally and here a - and here technology due diligence is a much more critical part of the decision - than in Norway.

For Atea: IT has become more important, and therefore cybersecurity has become more critical. Especially on the products, but also for companies where they will use the technology after the acquisition.

"If you had asked about cybersecurity when acquiring it for ten years, I would have said - I do not understand what you are asking about."

> "Cybersecurity has been on the agenda of management and boards in companies only in the last 3-4 years."
>
> Steinar Sønsteby, CEO Atea

4.2 Storebrand

The Storebrand Group is a leading player in the Nordic market for long-term savings and insurance. Storebrand offers pension, savings, insurance, and banking products to private individuals, businesses, and public enterprises. Storebrand has existed for 250 years and is Norway's largest private asset manager, with NOK 921 billion invested in more than 3000 companies worldwide. Storebrand's ambition is to build a world-class savings group supported by insurance. They offer life insurance products, property and casualty insurance, asset management and banking, to companies, public sector entities, and private individuals. Storebrand has about 40.000 corporate customers and 2 million individual customers and is Norway's largest private asset manager (*Storebrand*, n.d.).

The Chief Executive Officer (CEO) is responsible for the Storebrand Group's daily management. The Group's senior management consists of leaders of key business areas and functions in Storebrand.

Good corporate governance is vital to ensure that Storebrand can achieve its defined goals, including the best possible utilization of resources and good value creation. An in-house Corporate Governance committee, established in 2006, is responsible for ensuring good corporate governance practice across the Storebrand Group. The Storebrand Group works continuously on improving both the overall decision-making processes and the day-to-day management of the company. Storebrand directs and controls its activities in order to create value for its stakeholders. The dialogue with these stakeholders is a central part of Storebrand's corporate responsibility. The Board of Directors is responsible for the Group's management and monitoring of the administration of the Group. The Board has appointed four committees: The Strategy Committee, the Audit Committee, the Risk Committee, and the Remuneration Committee (*Storebrand*, n.d.).

4.2.1 Relevance for the research

Storebrand is relevant for this research because of a few significant acquisitions in the past years. They have a large investment in technology development internally.

4.2.2 The Interviewee

I conducted a qualitative semi-structured interview with Tore Lind, Head of M&A in Storebrand, in early November 2020.

The interviewee who was chosen for the research assignment was Tore Lind, as Head of M&A in Storebrand. As Head of M&A, he is responsible for all acquisitions and mergers in the business. He knows the business well after having held many other different financial positions in the company.

The interviewee has been involved in five acquisition transactions in the last three years. The company has acquired both companies and portfolios.

4.2.3 Organization of the Acquisitions

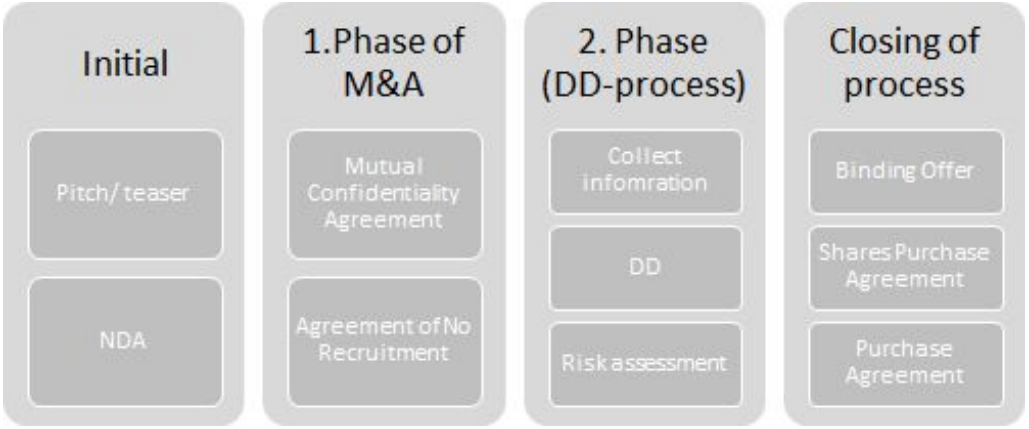
For Storebrand, the takeover process is based on five parts or phases.

The takeover process is demanding, and the process should not take too long. It can take 2 - 8 weeks, but preferably 2-3 weeks. Storebrand involves many people in the process and, in addition to the due diligence team, the relevant business area, the CFO, participates in taking care of the valuation. A legal team takes care of the contractual conditions. For larger projects, Storebrand uses external specialists related to Financial advice, legal advice, and negotiations.

Storebrand has at least a team of 8-10 people and can eventually reach up to 50-80 people who look at various company-specific and risk-based parts.

Storebrand has its own reliable environment within IT and digitization, which also contributes. They also have their own CISO (Chief Information Security Officer), which looks at cybersecurity, and the CRO (Chief Risk Officer) who looks at compliance with GDPR and cybersecurity. Storebrand believes that they have sufficient resources internally to take care of IT and cybersecurity for due diligence. But if there is a shortage of internal resources, they acquire external resources in various areas. External privacy lawyers are sometimes procured.

4.2.4 The Takeover Process



Storebrand has a structured course for the takeover process. The process is fourfold, and the acquisition part itself divides them into two phases.

Initially, the process starts with them getting a Pitch, a small teaser from someone who wants to sell. Alternatively, Storebrand's activity chooses its candidates based on an acquisition strategy. The strategy may be a desire to grow within a given business area. The process in the future is the same for both types of acquisitions.

If both parties find it of interest, they will enter into a Non-Disclosure Agreement (NDA). The NDA is a mutual obligation regarding confidentiality in the process. It usually also contains clauses not to recruit employees between the companies.

After this comes the first takeover phase, several potential buyers may be involved in this process, and all have limited access to information. If Storebrand is interested, it may result in an Indicative bid.

The next takeover phase is the due diligence phase. There are fewer actors in this section. The seller opens a computer room so that relevant buyers can gain knowledge about the company. Here is information about internal documents and routines about business matters, employees, conditions, GDPR, IT, cybersecurity, etc.

Sometimes Storebrand stops the process after findings in the due diligence process if the risk is greater than the company is willing to accept. It may happen that the risk is significant, but that Storebrand considers that it can handle the risk. In such cases, they go further in the process. The risk associated with reputation is significant, and it can lead to Storebrand leaving the buying process. The result after due diligence can lead to a final process.

Finally comes a Closing of the process. Storebrand makes a binding offer for the company and is entering into the final negotiations, Shares Purchase Agreement, and a definitive purchase agreement.

4.2.5 The Due Diligence Process

The purpose of due diligence is to uncover the robustness of the company, which is relevant to buy. Storebrand looks at the condition of the company, with all possible parameters. If Storebrand considers that the risk is manageable but still a vulnerability of the company, it is a parameter in the price negotiations. The most important thing is to safeguard and secure the values of the procurement. Still, secondarily, the risk identified in due diligence can be the consequence of the negotiation of a fair price.

The industry sets strict regulatory requirements. So a vital area in due diligence is regulatory risk, which licensing frameworks to deal with. But also disputes with customers or other suppliers and financial risk are essential aspects to consider.

4.2.6 Cybersecurity

Storebrand is dedicated to protecting the customers' personal data and personal privacy so that the information shall be safe. This includes all information that can be used to identify you personally, such as your national identity number, contact information, and information regarding the products you have purchased from Storebrand (Storebrand, n.d.).

Poor cybersecurity can give Storebrand a competitive disadvantage. The customer may lose confidence in the business and thus lose faith in the market as well. This is a self-regulatory process, which Storebrand tries to stay ahead of.

The board is concerned with cybersecurity. Every year, the governing documents are updated and approved by the board, which the company must comply with.

The interviewee has knowledge of the acquisitions in the company from the early year 2000, and the company has focused on IT technology at all times. Cybersecurity is, therefore, an essential part of the due diligence process. Storebrand uses internal resources to take care of this.

"If we detect large risks also related to cybersecurity, it can be a 'deal-breaker'"

Tore Lind, Head of M&A, Storebrand

4.3 Visma

Visma was founded in Oslo, Norway, through the merger of MultiSoft, SpecTec, and Dovre Information Systems in 1996. In 1997 and the financial crises, Visma was restructured, had a new strategy, and replaced most of the management and Board of Directors – and had 310 employees (Visma, n.d.).

Visma delivers software that simplifies and digitizes core business processes in the private and public sectors. With a presence across the entire Nordic region along with Benelux, Central and Eastern Europe, and Latin America, they are one of Europe's leading software companies. Visma continues its strong growth thanks in large part to increased demand for cloud accounting and e-invoicing solutions. In 2019 Visma has close to one million customers run their business every day, and more than 11.000 employees. Their revenue in 2019 was EUR 1.526 mill. The Visma group consists of over 200 companies across more than 20 countries worldwide. Our unique structure allows us to be close to the local markets while sharing world-class competence across the organization (Visma, n.d.).

Over 20 years of experience in software innovation – helping people work more efficiently – has made them who they are today; A leading European software provider with close to one million customers worldwide (Visma, n.d.).

Visma has themselves had data breaches, and one of them got much attention some time ago. Espen says that also Visma's shareholders came and had questions about this in the time after. The shareholders' interest contributes to giving more cybersecurity focus to the board, which gives the responsibility to the management. The focus in the top management helps IT and cybersecurity getting better support while doing their job.

"It is a great fear about this within our shareholders."
- Visma's Security director

4.3.1 Relevance for the research

Visma was selected as one of the three cases for this task, mainly because Visma is, compared to Norwegian businesses, a large company with 11.000 employees, and their business is primarily within IT and IT development. They are doing almost one acquiring case a week and are expecting 40 acquisitions this year. The C-level group sets the direction for the company and then sees which areas they need to strengthen. The business development section will check out these areas and then try to identify potential acquiring cases. Instead of buying one or two excellent companies, one of their strategies is to buy five "okay companies."

4.3.2 The interviewees

Visma contributed with two persons in the interview, an advisor from the business development section for the last four years, and the product security director. The advisor had worked with all types of due diligence in his role and was looking out for potential businesses.

Visma has, in the timing of the interview, 24 employees who work within cybersecurity and are particularly strong in application security.

4.3.3 Organization of the Acquisition

Visma carries out up to 40 acquisitions per year, so there are almost weekly acquisitions in the company. The company prioritizes more "fairly good" acquisitions rather than a few "very good" ones. A takeover is based on the companies evaluating having business values that Visma wants. There are strategic decisions about business development, and Visma sees in the market, whether there are interesting companies for acquisitions in relation to the business strategy.

There is a separate investor team that organizes the acquisitions and also makes the final assessments of which companies are acquired.

Visma has a conglomerate structure on the companies that are acquired. The power, control, and responsibility will remain with the acquired company. This also makes it easier to divest companies if the acquisition was not satisfactory. That said, Visma sells few companies, compared to what they buy. The assimilation of new companies is taken over time. With its cybersecurity expertise, Visma can onboard companies that do not have adequate cybersecurity.

Although the acquired companies have their own management, the branding of most companies is linked to Visma, so in this sense, Visma is affected if severe incidents occur.

4.3.4 The Takeover Process

The takeover process in Visma is divided into three stages; Pre, During, and Post.

In the **Pre-process,** information is gathered by the purchasing team for assessments. Security intelligence is activated if Purchasing is in doubt. The intelligence process is a demanding program and is, therefore, rarely implemented. The intelligence process looks at whether the products are trustworthy. Are there artifacts in the people and systems that cause concern?

Cybersecurity assessments of country risk can be done early in the process. This will include the risk of corruption in various countries.

Visma makes strategic decisions about business development and sees in the market if there are companies that are interested in acquisitions considering the business strategy. Safety assessment of land risk can come in early in the process, but this is also more strategic. This concerns, for example, the risk of corruption in various countries. Cybersecurity comes in if the companies are shortlisted.
If the companies are not tech companies, for example, engaged in production or pisciculture - cybersecurity is probably not as relevant to implement yet.

In the **"During-stage,"** the due diligence process takes place. There are clearly defined tasks in this section, which will help make the management equipped to make the acquisition and set the price. Visma also considers how the business or product should be organized and onboarded in this stage.

During the check of potential businesses to acquire, the cybersecurity team assists with due diligence, especially the tech due diligence. The impression the target firms leave the first times they talked and met decides how comprehensive cybersecurity due diligence Visma will do. Sometimes, asking the right questions could leave the certainty of the cybersecurity status.

After the due diligence process results, the tech and its cybersecurity are not necessarily decisive for the provision to buy or not. Most of all, Visma uses the information to set the price correctly and know if they should bargain, seeing that the costs of correcting deficiencies will be high after the acquisition. Also, they already start by submitting a plan for on-boarding the company to the conglomerate.

It is the investor team that makes the final assessments. If two different companies are considered equally "good," - cybersecurity can contribute to choosing.

In the **Post-section** of the acquisition, Visma's security program is further introduced. It is essential to know the vulnerabilities of the company and add the necessary expertise if necessary. Visma will assist the company in improving cybersecurity after the acquisition. When new companies are onboarded, Visma can withstand taking in products and companies with inadequate cybersecurity.

4.3.5 The Due Diligence Process

A separate information room is established in the due diligence process, where documentation about the company is entered. Visma does tech due diligence where they look at the business people's knowledge and technology. They are looking for eg competence deficiencies. Cybersecurity is one of many parts of the tech due diligence (YouTube video and book) - reference

When Visma looks at the technology, they focus on seeing what kind of technology they have, how it is structured, and whether individuals in the company are an addiction to the operation further.

4.3.6 Cybersecurity

Cybersecurity has gained more focus in society. Shareholders, customers, and management are also concerned about Visma's cybersecurity and follow up when security incidents occur. Awareness has increased and is as well crucial at the board level. There are many questions about security from many quarters.

Visma has gradually integrated cybersecurity in its risk management of acquisitions. The technical due diligence started right from the start 34 years ago. But cybersecurity has become more professional. Technical security reviews became more common five years ago. Previously it was focused on technical debt. Now it is also focused on cybersecurity.

Visma started to do the due diligence of cybersecurity about five years ago. This decision was made based on trends and needs. The cybersecurity threats became broader than before, and the focus on cybersecurity from the management, the board, the shareholders, and the customers have increased and almost doubled each of the following years.

The actual application security field has not been advanced enough on a worldwide basis until recent years that there has been some point in including us. Only now is it starting to get advanced enough that there is any point in doing tests and investigations of it. It has been quite right to just focus on technical debt for so long. Still, now Visma also needs to look at their cybersecurity and begin to smell whether they should start looking at their intelligence capabilities and chances of resisting attack. Whether they should carry out actual exercises on them as part of the due diligence. Visma discusses several things, but it is also vital that they do not make it too advanced.

Another question Visma usually asks is whether they have had a data breach and if so, will it be possible to look at the report to the local police? If the incident is reported to the police, it is a sign of great maturity in the organization.

If two different companies are considered equally "good," - cybersecurity can contribute to choosing.

Visma has a large cybersecurity team, and the reviews of the companies are partly very technical. The interviewee says that often some simple questions can reveal the level of cybersecurity. Questioning if there has been a security incidents and asking for access to reports of incidents to local police can say a lot. Being able to submit a review is usually a sign of great maturity. Another sign of cybersecurity maturity is asking about some of the latest attack vectors on a particular platform. If the company's cybersecurity department is aware of this, it is a sign of maturity. Very often, testing of the source code is also performed.

In due diligence of cybersecurity, Visma looks at the documentation that is available and assesses whether the company complies with the measures in the Security Development Life Cycle (SDLC). They also do source code testing and penetration testing. If Visma Finds information about this in the business, the risk is low. Application security is the most important focus within the cybersecurity field.

This, together with its own expertise in cybersecurity, means that Visma can take in companies that do not have satisfactory cybersecurity.

If it is a very important and strategic acquisition for Vimas, they will not save money on cybersecurity. The necessary resources will be used to ensure a good enough level of cybersecurity.

In some cases, Visma Bounty pays to check the cybersecurity of the companies that are acquired. If strategic decisions need to be made, very intrusive cybersecurity reviews are necessary. They hire the best "hackers'' in the world who are looking for vulnerabilities. For every vulnerability they find, the service must pay "bounties''. If the risk is very large, the cost for a month can be up to NOK. 750,000. When the price is so high, then there are very many gaps in the services. Doing these kinds of vulnerability controls changes behavior. The vulnerabilities that are discovered must be patched quickly. Otherwise, knowledge about the vulnerabilities will spread - and they can be exploited. This is not a regular penetration test, but much more demanding. There are few times Visma does this, but if the acquisition is very important, they do this intrusive job. Normally, the median price for Bounties is NOK 22,300 per year to detect vulnerabilities.

Cybersecurity is seldom what stops an acquisition if this is a business idea in general. Inadequate cybersecurity could affect the price of acquisitions. Visma follows up and measures the cybersecurity of the companies that have been acquired until Visma sees that the cybersecurity level has a necessary maturity.

> “We look at this as parenting. When a company has matured sufficiently, we can let go and it can “leave the nest””
> Espen Johansen, Product Security Director, Visma

4.4 Financial Reports

All the case firms deliver annual and financial reports to their existing and potential investors. It can be read how the previous year has been in both numbers and words from the CEO in these reports. To compare the firms together and to itself, I have found data from the annual reports from 2014 to 2019. These data will give some extra input and information about the case firms' focuses on acquisitions and cybersecurity. It also holds information about which acquisitions the case firms' did in the mentioned years.

	2014	2015	2016	2017	2018	2019
Atea	4	1	1	0	1	1
Storebrand	0	0	0	2	0	1
Visma	10	12	25	17	19	20

Table 4.1. Number of acquisitions mentioned in annual reports

	2014	2015	2016	2017	2018	2019
Atea	88	80	62	34	43	57
Storebrand	44	37	32	87*)	53	50
Visma	82	95	102	90	103	113

Table 4.2. How often "Acquisition" is mentioned in the Financial Report for the years 2014 to 2019.

Atea	2014	2015	2016	2017	2018	2019
Cybersecurity	0	0	0	0	0	0
IT Security	3	10	7	7	2	1
Information Security	0	0	0	1	0	2
Security	25	34	19	23	14	15
Privacy and GDPR	0	0	0	1	0	0

Table 4.3. How often words connected with "cybersecurity" are mentioned in Atea's Financial Report for 2014 to 2019.

Storebrand	2014	2015	2016	2017	2018	2019
Cyber Security/ Risk	0	0	0	0	1	0
IT Security	0	0	0	0	0	0
Information Security	2	2	3	10	5	7
Security	23	21	24	34	29	30
Privacy and GDPR	0	0	3	20	18	12

Table 4.5. How often words connected with "cybersecurity" are mentioned in Storebrand's Financial Report for 2014 to 2019.

Visma	2014	2015	2016	2017	2018	2019
Cyber Security	0	0	2	3	3	4
IT Security	0	2	3	1	1	1
Information Security	0	4	5	1	1	2
Security	6	18	28	8	9	17
Privacy and GDPR	0	1	4	3	2	5

Table 4.6. How often words connected with "cybersecurity" are mentioned in Visma's Financial Report for 2014 to 2019.

4.5 Cross-Case Analysis

In order to complete the cross-case analysis, findings from the firms' transcribed interviews were compared within the following categories: Their takeover strategy, the due diligence process, the integration process, and their cybersecurity knowledge and priority. Thus, in this section, information from the different case firms' financial reports will be compared and analyzed. Tables that summarize the empirical findings will be presented.

4.5.1 Takeover Strategy

All cases have a large focus on acquisitions in their financial reports and in the interviews. Everyone uses acquisitions for growth and to enter new markets. However, there is a big difference between how quickly they make acquisitions and how big the companies they acquire are.

Both Atea and Visma have written that they are making acquisitions as a part of their growth strategy and reaching new countries and markets. In the interviews, Atea and Visma stated that they strategically search for suitable firms to acquire, while Storebrand, on a larger scale, takes the opportunity when it comes their way.
Atea and Visma both do serial takeovers, which means they

There are some clear differences in how companies seek out acquisition situations. As Atea and Visma have acquisitions as a large part of their growth strategy, and they are making series acquisitions, they are actively looking for companies to buy. Visma explained how they set strategies for periods for what they are looking for and which markets they want to have growth in the future, then they are actively looking for companies that suit these markets. This can be technologies, industries, or areas, or countries. Atea has somewhat the same strategy, where they themselves lookout for companies to potentially buy. Visma, in particular, emphasized that they have certain precautions in the search for companies based on cybersecurity strategy. This can be to exclude companies with certain backgrounds or from certain industries.
Storebrand is not looking as actively with a similar strategy for what they will acquire in the future, but is looking for opportunities and is also sought out even from companies that may consider being acquired by Storebrand.

4.5.2 Due Diligence Process

All cases have a takeover process strategy that forms the way they do the takeover. This is quite similar for all cases, even though they present it in different ways. While Storebrand tells about their five stages, and Atea and Visma present the stages as three, they all present the same processes as parts of the stages.

All the cases do most of the due diligence themselves, but Atea and Storebrand also hire consultants, lawyers, and financiers to do some of the investigations. Atea said that they also in some cases, use technologists from other technology companies that have knowledge and expertise in investigating certain kinds of technology. This is especially if the companies they are going to do due diligence to have specific technology. It is especially one company they have used several times. This means that they know how to work and trust them to make good assessments of the technology.

Visma does everything themselves and has good strategies for how to carry out due diligence. Visma processes several due diligence every year. For every takeover, they assess to what level and detail the due diligence must be done. Therefore, they have good routines that are followed through due diligence that they know can be followed by their professionals.

For Visma's part, a cybersecurity assessment during the due diligence process is mainly done to tune the price of the company they plan to buy and to be able to make a good plan for the onboarding when the time comes.

Both the other two case companies have stated in the interviews that cybersecurity can "make or break" a deal and that a "no-go" during the assessment of cybersecurity can be a showstopper regardless of the price of the deal.

4.5.2.1 Due diligence Team

When due diligence is to be carried out, there is often a hurry. The company in question must be reviewed as best it can in a fairly short limited time. The team that does this is also crucial to get the most out of the due diligence process and show up in a short time with good routines and knowledge.

External teams
All companies use external teams for the due diligence process but in various size and scope.
Visma uses external teams for the largest and most important deals for financial due diligence. All other types of due diligence are done internally. The sizes of the teams vary on the size and importance of the deals.
Atea uses external teams for some technology and cybersecurity due diligence, and Storebrand uses external teams for legal, financial, and sometimes external advisors as a corporate bank. They use internal teams also, and the team working in front of the deal could be 50-80 persons, where the goal is to know as much as possible, and for example, GDPR and privacy were cited.

4.5.3 Integration Process

The integration process is an important phase for all of them. At this stage, they can make up for poor cybersecurity if they found out about this during due diligence.

Atea is wasting technology. Visma does not fully integrate but keeps them as separate companies under the Visma structure, but helps them build stronger cybersecurity if needed.

Visma can buy companies with poor cybersecurity as they have the advice and resources and a good onboarding strategy to build cybersecurity well enough. They have good general plans for integrating acquired companies, which involves running them through the Visma Security Program. They do this with all the companies within a year of the company being acquired. The time before they go through the security program depends on how important the newly acquired company is for Visma and how bad the cybersecurity company already has.

4.5.3.1 Conglomerate

While Atea and Storebrand are primarily focused on horizontal and vertical acquisitions to broaden their presence in their existing markets, Visma also does conglomerate and uses the conglomerate structure as part of the risk aversion strategy, also for cybersecurity risks. In this way, they have found out not Visma as the whole group will be affected by a security incident.

4.5.3.2 Scrape Everything

Atea integrates the companies into its own company. They retain little of the technology in the acquired companies but use the employees' expertise, the customers, and xxxx in the company. The acquired company will use Atea's technological solution.

4.5.3.3 Synergy Effects

Visma uses this synergy effect by having their Visma Security Program, which they run all their acquired firms through after the takeover.
Both Atea and Visma provide this for their acquired firms, which gives them a better competitive advantage in the market.
The cybersecurity acquisition strategy model of Visma works out because they have the knowledge on-site in the group and have the economy to implement and strengthen cybersecurity inside the acquired firm. This model will not be working out for firms not having the knowledge or the economy.

4.5.4 Cybersecurity

All three cases have increased the focus on cybersecurity in recent years. Atea, which is a more pure IT company, has worked with cybersecurity for several years, but professionalism has increased significantly in recent years. All the cases also say that this is due to increased attention on a general basis, including in the media. Events are also described in the media. In addition, cybersecurity comes to the table of management and the board. This, of course, increases competence and capacity in the field. All companies have a cybersecurity or security department and a Chief Information Security Officer (CISO). These roles and departments are included in the due diligence process for cybersecurity. Sometimes all the companies needed special expertise in the field and then hired the necessary resources.

The interviews showed a big difference between the three companies: Cybersecurity could be a show stopper for two of the companies, while one of the companies was based to a small extent on using the technology of the acquired company, and thus cybersecurity was less critical. This company could also invest considerable resources in improving cybersecurity if the company was of great strategic importance to acquire and if they were to bring the company's technological solutions with it in the future.

As Sønsteby in Atea said, the question of whether they were looking at cybersecurity prior to acquisitions had he not understood what he was asked about or why. This clarifies what change has taken place in terms of both focus and how seriously cybersecurity is taken in just ten years. In financial reports, it is only five years back in time, and only there is a clear change in focus. This tells us something about how the management, the board, and investors and shareholders think about cybersecurity. To a greater extent now than before, they consider it an important area to focus on.

The risk that a security incident may go beyond the reputation of the company is quite large. Especially if the media starts writing about the security incident. Often the company itself goes out with information that they have had a security incident, in some time after the incident has occurred and they have control over the situation and cleaned up the incident. Since one can not expect to never experience an event, it will show strength to go out with this information and handle the event. Nevertheless, it can seem sweaty negatively in the media and have a negative impact on reputation. It was nevertheless highlighted how the handling of the security incident Hydro experienced in the spring of 2019 made the shareholders trust them throughout the incident, even though it cost them dearly and they lost weeks of normal operations.

Taking over operations for other companies is reminiscent of acquisitions (outsourcing). Atea takes over tasks for essential parts of the IT infrastructure for customers. Even if it is not an acquisition, the risk associated with the IT part will be similar. Atea needs to know the quality of the systems and do due diligence. Serious security incidents for the customer will affect Atea's reputation.

Chapter 5 - Discussion

In this Chapter, I will extract the most important findings from chapter 4.5 Cross-Case Analysis and discuss them in connection with the literature from the literature review. Some of the conclusions made in Chapter 4.5, where the cases were cross-case analyzed, will change somewhat in light of previous research found in the literature review. The topics discussed in this chapter are the due diligence process, integration of acquired firms, and how the cybersecurity level is assessed. The cybersecurity level will be seen in the perspectives of the Capability Maturity Model Integration (CMMI) presented in Chapter 2.3 as the framework for this study.

5.1 Due Diligence Process

The three companies all have a predefined process for the acquisition. The procedures are relatively similar. Hirschheim and Mehta (2004) and Feix (2020) also define that acquisitions with a subsequent integration process can be roughly divided into the following phases pre-merger, merger, and post-merger (Hirschheim and Mehta 2004). Feix (2020) uses the same three phases in his end-to-end merger and acquisition process design, just using the terms embedded merger and acquisition strategy for pre-merger, the transaction management for the takeover, and integration management for post-merger.

What do they assess when they carry out due diligence of the target firm.
Aabø-Evensen states due diligence also increases the probability that the buyer achieves synergies that may motivate the acquisition (2011).

As Feix (2020) says, due diligence intends a consistent, robust, and stress-tested proof-of-concept of the target company. The interviews with the cases confirm that their due diligence process is similar to Feix (2020) description. Gathering large teams and quickly assessing most possible of the target firms' information within their chosen fields of subjects for only a few weeks. Feix (2020) mentions that the team can be both in-house or consultants from outside the group. For cybersecurity, the case firms mostly use in-house professionals, but Atea and Storebrand also supplement consultants or technology companies outside their group. External consultants are specially hired for the legal parts of cybersecurity and privacy, where the laws have become more pointed and stricter in recent years, which in turn has increased in importance.

The price of the acquisition depends on the values of the company being acquired. Berk and DeMarzo (2017) begin explaining the takeover process by establishing how the Acquirer determines the initial offer. The Acquirer will have to value the Target firm and quantify and discount the value-added as a result of the takeover. The valuation of the Target firm can be calculated in several different ways. Some of the most usual might be using a multiple based on comparable firms, an estimate of value including accurate analysis of the operational aspects and the ultimate cash flows the deal will generate (Berk & DeMarzo, 2017). Once the Acquirer has completed the valuation process, it will make a tender offer - a public announcement of its intention to purchase the Target firm.

In case that the companies take over ICT systems, which are an essential value in the companies that are acquired. The value of the target firm will be affected by the quality of cybersecurity in the ICT systems. This can be compared to the benefits such as Allen, Brealey, and Myers (2017) gives examples of occasions where the takeover achieves gains. Still, the Acquirer nevertheless loses because it pays too much for the Target firm. The buyer might overestimate the value of stale inventory or underestimate the costs of renovating old plants and equipment. It may also overlook the warranties on a defective product. The Acquirer needs to be particularly careful about environmental liabilities. If there is pollution from the Target firm's operations or toxic waste on its property, the cost of cleaning up will fall on the Acquirer. This is a literal wording from Allen, Brealey, and Myers (2017) with sustainability in mind, that can also be seen figuratively with other ways of bringing a lousy reputation.

The three companies all have a predefined process for the acquisition. The procedures are relatively similar. Hirschheim and Mehta (2004) and Feix (2020) also define that acquisitions with a subsequent integration process can be roughly divided into the following phases pre-merger, merger, and post-merger (Hirschheim and Mehta, 2004). Feix (2020) uses the same three phases in his end-to-end merger and acquisition process design, just using the terms embedded merger and acquisition strategy for pre-merger, the transaction management for merger, and integration management for post-merger.

The price of the acquisition depends on the values of the company being acquired. Berk and DeMarzo (2017) explain the takeover process by establishing how the Acquirer determines the initial offer. The Acquirer will have to value the Target firm and quantify and discount the value added as a result of the takeover. The valuation of the Target firm can be calculated in several different ways. Some of the most usual might be using a multiple based on comparable firms, an estimate of value including accurate analysis of the operational aspects and the ultimate cash flows the deal will generate (Berk & DeMarzo, 2017). Once the Acquirer has completed the valuation process, it will make a tender offer - a public announcement of its intention to purchase the Target firm.

5.1.1 Looking for Lemons

The companies have different strategies for acquisitions and how they seek and find acquisition opportunities, but it has been used as a method for growth for all companies in the study everyone. This means that they are particularly observant of the risks associated with acquisitions. Successful growth following an acquisition depends on the integration going well and that there are no surprising risks, "lemons" in the acquired company. A "lemon" can be an incident that occurred several years ago, as a money laundering or a data leak.

All three companies used as cases in this study, confirm that they examine the companies' information security before making an acquisition. The technology in the company is thoroughly examined before the acquisition.

All case companies now have a strong focus on cybersecurity. This is a change for all of them, as the focus on cybersecurity has increased significantly in recent years and continues to grow. Especially when it comes to privacy and security of personal information, there has been a sharp increase in focus and severity among the case companies in recent years. This has happened after it became known that the new privacy regulation (GDPR) came and especially after it was introduced and implemented. There has also been a change in how serious cybersecurity is considered in the company as a whole. The threat picture and media focus for cybersecurity significantly affect the companies. The companies notice that shareholders, the board, and management follow how cybersecurity changes internally and externally in the company. The seriousness of their focus on cybersecurity has increased and is more on a par with how, for example, breaches of money laundering rules are assessed.

IT can, does, and should play a significant factor in making or breaking a takeover deal (Gleich et al., 2018). From the interviews the theses have found the same experiences as both Storebrand and Atea says in the statements below.

"If we detect large risks also related to cybersecurity, it can be a 'deal-breaker'"
Tore Lind, Head of M&A, Storebrand

"Is it 'No-go' on Tech due diligence, is it showstoppers regardless of price,"
Steinar Sønsteby, CEO Atea

5.1.2 Pricing

The study shows that the case companies are worried about acquiring a built-in "lemon" in technology. The costs of ensuring good cybersecurity and of a security incident when acquiring companies are dissuasive. If cybersecurity is not adequate, it could be a showstopper for two of the three companies interviewed. Above all, companies' most important thing is to know the risks with inadequate cybersecurity when determining the price and deciding on the procurement.

In the cases Atea considers that if the results are possible to live with, it impacts the price. The interviewee in Atea had examples of acquisitions being stopped due to tech-due diligence. Storebrand says in the interview that the level of Cybersecurity can be used to negotiate pricing. Visma states that cybersecurity is seldom what stops an acquisition if this is a business idea in general. Inadequate cybersecurity could affect the price of acquisitions.

Results from due diligence, including results related to Cybersecurity seem to affect the price. Discussing price is a way to handle "lemon". However, this may be affected by the strategy for acquisitions and the extent to which the IT systems will be used in the business in the future.

5.2 Integrating the Acquired Firm

Aabø-Evensen says that due diligence also increases the probability that the buyer achieves the synergies that may motivate the acquisition (2011). As due diligence of the target firm's cybersecurity is mainly to understand how to integrate the firm within the group, the integration also increases the probability of success. Visma sets the post-merger strategy when they conduct due diligence. This post-merger strategy is mainly to onboard the acquired firm the best way, gaining most of the synergy effects, and getting the potential value creation first possible.

Atea chooses to use synergy effects differently. By integrating and onboarding the acquired firm into all of Atea's systems, they do not need to fix their cybersecurity in a better way. They know their infrastructure and technology are strengthened in cybersecurity, and by using this for their whole group, they only have one infrastructure to focus on.

There is a big difference between the case companies on how the companies that have been acquired are integrated. The similarity is that integration is the most affected part of the procurement process in terms of the results of the cybersecurity surveys. One of the case companies does onboarding by running Target firm through their security program to ensure that cybersecurity has a good enough level according to their standard. Also, this company maintains, to a greater extent, a conglomerate structure within the company, which means that they retain the Target company's infrastructure and existing technology. One of the other case companies "rejects" the technological infrastructure in the Target firm and places them in their existing infrastructure instead.

"We look at this as parenting. When a company has matured sufficiently, we can let go and it can "leave the nest""

Espen Johansen, Product Cybersecurity Director Visma

5.2.1 Conglomerate

As Berk and DeMarzo (2017) explain, a takeover can be horizontal, vertical, or conglomerate. The cases in this thesis have experiences in all of them. While Atea and Storebrand primarily focus on horizontal and vertical, Visma also does conglomerate and uses the conglomerate structure as part of the risk aversion strategy and cybersecurity risks. In this way, they have found out not Visma as a whole will be influenced by a security breach.

5.2.2 Synergy effects

The smaller firm's synergy effects of being a part of a larger group also give them a "suddenly" competitive advantage. They get the larger groups competence in cybersecurity, as an example. This is consistent with Berk and DeMarzo (2017) which state that one of the synergies that can justify the takeover is that a larger group will be able to enjoy the savings from producing on larger scales. Cybersecurity is complicated because of its rapid change, and it requires a lot to keep up with threats and trends. With a larger group, the group can pose with an expert team in cybersecurity to support

the smaller firms acquired. Visma uses this synergy effect by having their Visma Security Program, which they run all their acquired firms through after the takeover.

Brealey, Myers, and Allen state larger groups are also acquiring many small firms because they can prove to have a missing ingredient necessary for the Target firm's success (2017). This missing piece can sometimes be better cybersecurity or a technical infrastructure with more strength. Both Atea and Visma provide this for their acquired firms, which gives them a better competitive advantage in the market.

An Acquirer might be able to add economic value to the Target firm, and by this value, create further synergies (Berk & DeMarzo, 2017). One of these additional synergies that were seen in the cases was that the Bidder had valuable knowledge within cybersecurity and therefore could strengthen the Target firm's cybersecurity after the takeover process. This was, in some of the takeover cases, the reason they could do the takeover. It gives the Target firm a gain, which can increase the level of cybersecurity. This can help the acquired firms to reach new markets.

The acquisition strategies of all three companies are to increase the market share within their industry. Increased market shares again increase the opportunity for new customers, who may assume that the largest supplier is the best choice. All cases use acquisitions as a strategy to reach new markets, also in new countries.
Berk and DeMarzo (2017) also state monopoly gains as a reason to takeover the Target firm. In Norway, the Norwegian Competition Authority conducts thorough investigations to ensure that the market is not monopolized, as seen in an example where Schibsted tried to acquire Nettbil (Weldeghebriel, 2020). This could instead be translated to take a larger piece of the industry.

The cybersecurity acquisition strategy model of Visma works because they have the knowledge on-site in the group and have the economy to implement and strengthen cybersecurity inside the acquired firm. This model will not be working out for firms not having the knowledge or the economy.

5.2.3 "Scrape Everything"

Atea integrates the companies into its own company. They retain almost none of the technology in the acquired firms. The acquisition is attractive because of the target firm's employees' expertise, customers, knowledge, processes, and reputation. The acquired company will use Atea's technological solution.

5.3 Cybersecurity

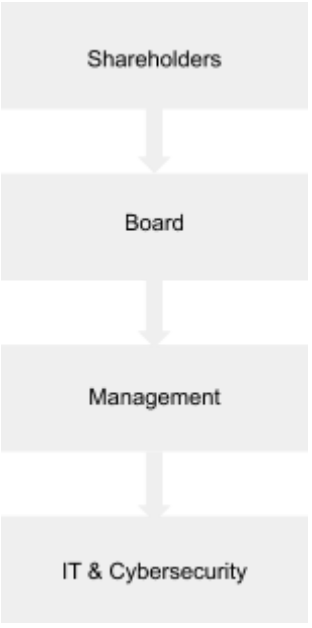
Due diligence is used to assess the firm's maturity in cybersecurity, and if the level of maturity is satisfactory, the company can be incorporated within their group.

Unsatisfactory cybersecurity can today affect the values of a company. Before committing to a takeover, managers usually conduct due diligence (Cullinan, Le Roux, & Weddigen, 2004; Perry & Herd, 2004; Rosenbloom, 2002). By reviewing the target firm's financial statements and anything else deemed material, they try to confirm the facts about the firm's ability to realize value from the takeover. Because they identify and assess the risks associated with takeovers during due diligence, they gain access to private information about the takeovers risk level.
Therefore, Cybersecurity should today be an essential part of assessing the risk.

In the interview Visma says that being able to submit a review is usually a sign of great maturity. Another sign of cybersecurity maturity is asking about some of the latest attack vectors on a particular platform. If the company's cybersecurity department is aware of this, it is a sign of maturity. Very often, testing of the source code is also performed.

Visma follows up and measures the cybersecurity of the companies that have been acquired until Visma sees that the cybersecurity level has a necessary maturity.
Visma does not describe a specific method for measuring maturity for Cybersecurity, but they use their own experience to assess maturity for potential companies before acquisitions. The cybersecurity team has various questions based on their own experience that provide indications of to what extent the company has satisfying cybersecurity.

A possible improvement in the assessment of maturity of Cybersecurity is to use a maturity model to measure Cybersecurity level, like Capability Maturity Model Integration (CMMI) (the Software Engineering Institute (SEI), 2008). There are also several other maturity models in the market.



5.3.1 Increasing Trend

It has been seen as an increase in the focus of cybersecurity in all of the case firms, and it also shows in the literature review as a growing trend. One of the reasons for this increasing trend is that the shareholders are starting to worry about a security incident's potential implications on the share price.

> "Cybersecurity has been on the agenda of management and boards in companies only in the last 3-4 years."
>
> Steinar Sønsteby, CEO Atea

> *"It is a great fear about this within our shareholders."*
>
> Visma's Product Security Director

5.4 Limitations of the Study

As written in Chapter 3 Method, there are several potential limitations of the study. This chapter will discuss which limitations are most relevant for this study and why it is essential to consider the limitations before concluding. I have already reflected on some limitations and assumptions in the method chapter.

- The study is based on a multiple-case study. Due to the limited availability of the interviewees, only a single interview was conducted per interviewee. This restricted the interviewers' opportunity to ask follow-up questions as they already had a set of predefined questions to go through. Thus, the interviewers might have lost details that were essential to understanding the concepts discussed in the interviews fully.
- The coding can have both a simplifying and a limiting implication on the inductive method. As pointed out by Gioia in the paper of Gehman et al. (2018), using the coding methodology too rigorously might have removed tacit and dynamic elements from the findings.
- The interviews have been done with different kinds of roles per case. The firms themselves have decided which position would be most suited for the case and Different roles, different organizations can affect what information the interviewees provide. The context in which they provide the information may also affect the outcome. The interviewer and the interviewees have different points of view and understanding and this can affect how the information is interpreted. There is a danger that information will be taken out of context or misunderstood.
- The interviewee knew in advance what the topic of the interview should be and what research question the assignment should answer. This may have affected whether they wanted to be interviewed and what focus they themselves had during the interview.
- Since the interviews were conducted in Norwegian, it was necessary to translate the quotes used from the transcriptions to English. Consequently, some of the wording may have been lost in translation. However, to ensure the validity of the translated quotes, they were emailed to the corresponding respondents, allowing them to cross-check the translation.

5.4.1 Credibility

The study is conducted by one interview with each case representative during the autumn of 2020. One of the techniques to increase credibility is to prolong the engagement of the interview respondent (Lincoln & Guba, 1985). Factors such as fear of negative publicity can have affected the answers given by the respondents (Halldorsson & Aastrup, 2003).

5.4.2 Transferability

Cybersecurity is a relatively new area to include in due diligence, and there are both shortcomings in the literature and a lack of experience in the companies. This means that the way cybersecurity is assessed in companies can differ from industry to industry and from company to company. Suppose other companies had been included in the study, either from another sector, with a different size, with other owners, or additional

cybersecurity expertise. In that case, the results could have been different from this study.

As this is a new trend and a qualitative study has been done of three companies, it is possible that the results would have been entirely different if it had been

5.4.3 Dependability

The dependability aspect of a research paper is concerned with whether the authors would reach the same conclusions if they could make the same observations twice (Lincoln & Guba, 1985). The data collection has been affected by the time and setting in which it was collected. Connecting the data to the theoretical frameworks has created comparability across the cases. Peer debriefing sessions have further been utilized to discuss the relation between the collected data and findings.

5.4.4 Confirmability

Working with cybersecurity and privacy, both as a consultant and building technology tools to help startups get better cybersecurity, I am interested in finding results saying cybersecurity is important for startups and smaller firms if they want to be acquired. It might also be the case firms who participated in the study have an interest in showing how great cybersecurity they have. At least, it is understandable companies with more lousy cybersecurity did not want to say so in research that will be published.
Therefore it is important that the findings are solely based on the data itself, and not the opinions of the authors. To mitigate this risk peer debriefing has been a useful tool.

Chapter 6 - Conclusion

The research question this thesis was supposed to answer is:

Question 1: *How does the Bidder assess the Target firm's cybersecurity before giving a bid?*

Question 2: *How relevant is the Target firm's level of cybersecurity for the takeover decision?*

In the study of this master's thesis, I have discussed and found answers to what drives the case companies' acquisitions of other companies, what they investigate before the acquisitions, how they conduct the investigations, and what impact the findings about the companies' cybersecurity level have on the acquisition decision and on the acquisition process in general.

6.1 Implications

The interesting findings and implications of this study is how its results affect startups and scale-up businesses, since these might strive to be acquired.

The findings in this master thesis may have a bearing on groups that have acquisitions as part of their strategy for growth. Cybersecurity is considered important in the due diligence of an acquisition by all companies in the study. Two of the three companies considered weak cybersecurity as an acquisitional deal breaker. The level of cybersecurity does affect the offer price in most cases. The state of cybersecurity also affects how the acquirer chooses to integrate the acquired company's technological infrastructure, which has a range of implications, including acquisition and integration costs - as well as the pricing of the acquisition.

It is also notable for smaller companies and startups aiming to be acquired. Cybersecurity is usually not the first priority in a startup. There are many tasks at hand; developing the idea itself, and other operational tasks, such as finance and market, must be prioritized. Cybersecurity usually lands further down the list of priorities. Such start-up companies may find the implications of this thesis useful and may see the benefit of putting cybersecurity higher on the priority list in an early stage of developing the business.

Based on the findings in the thesis, it is clear to see that startups with satisfactory cybersecurity can demand a higher price for the company. Startups can risk not being able to sell their business, if the products or services do not have satisfactory cybersecurity. Improving security is not always easy if the design does not include cybersecurity from the start. This can be a motivation to include cybersecurity in the development of products and services right from the get-go.

Over the last six years, the focus on cybersecurity and data privacy has increased significantly. This applies in general, both to start-up companies and large companies, but there could also be significant consequences in an acquisitional situation, both for the buyer and the seller, if cybersecurity is not satisfactory.

Through a literature study, a literature gap was discovered in research on the topic. I have conducted a qualitative abductive survey with semi-structured interviews of managers in three major Norwegian companies. Based on this, I have discussed and concluded what is standard in the industries as of today. I have also concluded how the findings affect both acquirer and acquiree - often entrepreneurial companies with a plan to be acquired. In this way, the study contributes to entrepreneurial business development and technology management.

6.2 Further Research

With very little research done in this area so far, there are many opportunities for further research. Here I will come up with some themes and approaches that I, after my study, view as ripe for further examination.

6.2.1 Quantitative study

My qualitative research says that at least some firms are assessing a firm's cybersecurity in due diligence, and use the results from this assessment to negotiate acquisition terms or to decide whether or not to acquire the target.

A quantitative study into the subject would certainly be interesting, yielding results with a greater breadth. This may include quantitative studies with several Norwegian companies, both of smaller and larger companies. International studies would also be of great interest.

6.2.2 Comparisons

A comparison of different businesses is another interesting approach. It may be relevant to conduct studies from both the buyer's and the seller's side. For example, is there a difference between small and large companies being the acquirer? Studies from the viewpoint of startup companies (often the acquiree) could also be of interest.

An international study, with analyzes of whether different countries have different assessments of cybersecurity during the acquisitional phase, would be particularly interesting. What are the different practises between the countries, and are there differences based on the different countries' legislations for privacy or cybersecurity?

Another engrossing angle would be a look at the differences in the various industries and how they value cybersecurity due diligence in an acquisitional process.

6.2.3 ESG

Environmental, social, and governance criteria have increased in importance and attention, both from investors, boards, and customers. Cybersecurity is a natural part of both the social and governance criteria. The environmental part of ESG has got the most attention, and there has been a lot of research about ESG and investments. It would be interesting to look at cybersecurity and investments from the angle of the social and governance parts of ESG, and furthermore how ESG models can be used to measure cybersecurity.

6.3 Limitations

Being limited by both time, experience and resources, this study probed a relatively small sample at a singular point in time. The small sample size did not allow me to generalize the findings presented in this study. Thus, I suggest that further studies should aim to replicate and nuance my findings with larger samples.

The study is based on a multiple-case study. Due to the limited availability of the interviewees, only a single interview was conducted per interviewee. This restricted the interviewers' opportunity to ask follow-up questions as they already had a set of predefined questions to go through. Thus, the interviewers might have lost details that were essential to understanding the concepts discussed in the interviews fully.
The coding can have both a simplifying and a limiting implication on the inductive method. As pointed out by Gioia in the paper of Gehman et al. (2018), using the coding methodology too rigorously might have removed tacit and dynamic elements from the findings.
The interviews were done with different kinds of roles per case. The firms themselves have decided which position would be most suited for the case. Different roles or different organizations can affect what information the interviewees provide. The context in which they provide the information may also affect the outcome. The interviewer and the interviewees have different points of view and understanding, and this can affect how the information is interpreted. There is a danger that information will be taken out of context or misunderstood.
The interviewee knew in advance what the topic of the interview should be and what research question the assignment should answer. This may have affected whether they wanted to be interviewed and what focus they themselves had during the interview.
Since the interviews were conducted in Norwegian, it was necessary to translate the quotes used from the transcriptions to English. Consequently, some of the wording may have been lost in translation. However, to ensure the validity of the translated quotes, they were emailed to the corresponding respondents, allowing them to cross-check the translation.

References

Aabø-Evensen, O.K. (2011). *Om oppkjøp av selskaper og virksomhet : en praktisk tilnærming til prosessene, verktøyene og eksemplene.* Universitetsforlaget.

Agrawal, & Jaffe. (2001). The Post Merger Performance Puzzle. Advances in Mergers and Acquisitions 1. 59. 10.2139/ssrn.199671

Akerlof, G. A. (1970, Aug). The Market for "Lemons": Quality Uncertainty and the Market Mechanism. *The Quarterly Journal of Economics*, *84*(3), 488-500.

Amoroso, E. (2007). *Cyber Security Ch. 3 - The Effects of Cyber Attacks*. AT&T Inc. https://dumitrudumbrava.files.wordpress.com/2012/01/cyber-security.pdf

Andrews, W. J., & White, J. E. (2017). Digital due Diligence: Four Questions to Ensure Your Organization has the Right Cyber Insurance Coverage. *Risk Management 64*, *02*(2017), 30-34. https://search.proquest.com/docview/1881388578?accountid=12870

Arcuri, M. C., Brogi, M., Gandolfi, G., & Citeseer. (2014). The effect of information security breaches on stock returns: Is the cyber crime a threat to firms? In European Financial Management Meeting.

Atea. (n.d.). Atea. Retrieved November 10, 2020, from www.visma.com

Atea. (n.d.). *About Atea*. Atea. Retrieved desember 1., 2020, from https://www.atea.com/about-atea/

Atea. (n.d.). *Atea Corporate management*. Steinar Sonsteby. Retrieved November 7, 2020, from https://www.atea.com/about-atea/corporate-management/steinar-sonsteby/

Atea. (2015). *Annual Report 2014*. Financial Reports Atea. Retrieved 11 29, 2020, from https://www.atea.com/media/2091/atea_annual_report_2014.pdf

Atea. (2016). *Annual Report 2015*. Financial Report Atea. Retrieved 11 29, 2020, from https://www.atea.com/media/2296/atea_annual_report2015_interactive.pdf

Atea. (2017). *Annual Report 2016*. Financial Reports Atea. Retrieved 11 29, 2020, from https://www.atea.com/media/2425/atea-annual-report-2016-interactive-version.pdf

Atea. (2018). *Annual Report 2017*. Financial Reports Atea. Retrieved 11 29, 2020, from https://www.atea.com/media/2511/atea_annual_report_2017_interactive.pdf

Atea. (2019). *Annual Report 2018*. Financial Reports Atea. Retrieved 11 29, 2020, from https://www.atea.com/media/2568/atea_annual_report_2018_interactive.pdf

Atea. (2020). *Annual Report 2019*. Financial Reports Atea. Retrieved 11 29, 2020, from https://www.atea.com/media/2714/atea_annual_report_2019.pdf

Ayyagari, M. R. (2019, June). Efficient Driving Forces to CMMI Development using Dynamic Capabilities. 7. 10.5120/ijca2019919024

Baker, S. (2017). Cybersecurity Becoming Big ESG Concern; Cost of Breaches Puts Issue at Forefront of Asset Owners' Agenda.

Berk, J., & DeMarzo, P. (2017). *Corporate Finance* (4. ed.). Pearson Education Limited.

Blaauw, H. (2019). *M&A en praktisk innføring*. Universitetsforlaget.

Boye, K., & Meyer, C. B. (2008). *Fusjoner og oppkjøp*. Oslo: Cappelen akademisk.

Brealey, R., Myers, S., & Allen, F. (2020). *Principles of corporate finance*. McGraw-Hill Education.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, *11*, 431-448.

Canongia, C., & Mandarino, R. (2014). *Cybersecurity: The New Challenge of the Information Society*. 10.4018/978-1-4666-4707-7.ch003

Cate, F. H. (2008). Information Security Breaches: Looking Back & Thinking Ahead. https://www.repository.law.indiana.edu/facpub/233/

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: capital market reactions for breached firms and Internet security developers. *Int. J. Electron. Commer*, *9*(1), 69-104.

Choong, P., Hutton, E., Richardson, P. S., & Rinaldo, V. (2017). Protecting the Brand: Evaluating the Cost of Security Breach from a Marketer's Perspective. *Journal of Marketing Development and Competitiveness*, *11*(1:59).

Coller Capital. (2017). *Global Private Equity Barometer*. https://www.collercapital.com/coller-capital-global-pe-barometer-summer-2017

Committee on National Security Systems (CNSS). (2010). National Information Assurance Glossary. *Instruction*, *No. 4009*. http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014, 10). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13-21. https://www.proquest.com/docview/1638205509?accountid=12870

Cullinan, Weddingen, & Le Roux. (2004). When to walk away from a deal. *Harvard Business Review*. https://hbr.org/2004/04/when-to-walk-away-from-a-deal

Eckstein, H. (2002). *Case study and theory in political science.* Sage.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review*, *14*(4), 532-550.

Erlandson, K. M., Harris, E. L., Skipper, B. L., & Allan, S. D. (1993). *Doing naturalistic inquiry: A guide to methods*. Sage.

FBI. (2019, April 22). *IC3 Annual Report Released*. fbi.gov. Retrieved November 10, 2020, from https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219?fbclid=IwAR10d3EfWLGX6E8iSJDgPNZq1OBpCIjWOD47IV2W9jdeNZxOhzUVH8TE96g

Feix, T. (2020). *End-To-End M&a Process Design*. Springer Fachmedien Wiesbaden GmbH.

Finkle, J. (2017). *St. Jude releases cyber updates for heart devices after U.S. probe*. Reuters. Retrieved November 15, 2020, from https://www.reuters.com/article/us-abbott-stjude-heart-idUSKBN14T1WT?fbclid=IwAR38qEt9EGGkhD82YgvginSxDFzRC-eoaHk2TtJ96Wd9VIse0o0SDu1QAFI

Flick, U. (2015). *Introducing research methodology: A beginner's guide to doing a research project*. Sage.

Fortune 500. (n.d.). *Fortune 500*. Retrieved November 15, 2020, from https://archive.fortune.com/magazines/fortune/fortune500_archive/full/2005/?fbclid=IwAR38qEt9EGGkhD82YgvginSxDFzRC-eoaHk2TtJ96Wd9VIse0o0SDu1QAFI

Galvan, J. L., & Galvan, M. C. (2017). *Writing Literature Reviews A Guide for Students of the Social and Behavioral Sciences 7th edition*. https://www.routledge.com/Writing-Literature-Reviews-A-Guide-for-Students-of-the-Social-and-Behavioral/Galvan-Galvan/p/book/9780415315746

Garfinkel, S. L. (2012, June). The Cybersecurity Risk. 10.1145/2184319.2184330

Garg, A., Curtis, J., & Halper, H. (2003, May). Quantifying the financial impact of IT security breaches. 10.1108/09685220310468646

Gehman, J., Glaser, V. L., Glaser, K. M., Gioia, D., Langley, A., & Corley, K. G. (2018). Finding theory–method fit: A comparison of three qualitative approaches to theory building. *Journal of Management Inquiry*, *27*(3), 284-300.

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational research methods*, *16*(1), 15-31.

Gleich, R., Kierans, G., & Hasselbech, T. (2018). *Value in Due Diligence : Contemporary Strategies for Merger and Acquisition Success*. Routledge.

Goforth, C. R. (2001). Technology Due Diligence--The Need for and Benefits of Technology Assessment in Connection with Investment in High-Tech Companies. *Rutgers Computer & Technology Law Journal*, *27*(2), 165-371. https://doi.org/info:doi/

Gole, W. J., & Hilger, P. J. (2009). *Due diligence – An M&A value creation approach*. Wiley.

Guba, E. G., & Lincoln, Y. A. (n.d.). Fourth generation evaluation. *Newbury Park*, (CA: Sage).

Guo, Y., Spínola, R. O., & Seaman, C. (2014). Exploring the costs of technical debt management – a case study. *Empirical Software Engineering : an International Journal*, *21*(1), 159-182. https://doi.org/10.1007/s10664-014-9351-7

Halldorsson, A., & Aastrup, J. (2003). Quality criteria for qualitative inquiries in logistics. *European Journal of Operational Research*, *144*(2), 321–332.

Hinz, O., Nofer, M., Schiereck, D., & Trillig, J. (2015). The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management*, *52*(3), 337-347.

Hirschheim, R., & Mehta, M. (2004). A framework for assessing IT integration decision-making in mergers and acquisitions. *37th Annual Hawaii International Conference on System Sciences,. Proceedings of the, Big Island, HI*, 264-274. https://www.computer.org/csdl/proceedings-article/hicss/2004/205680264c/12OmNzvQHZd

Hydro. (2020, October 14). *Cyber-attack on Hydro*. hydro.com. Retrieved November 10, 2020, from https://www.hydro.com/en/media/on-the-agenda/cyber-attack/

ICO. (2019). *Statement: Intention to fine Marriott International, Inc more than £99 million under GDPR for data breach*. ico.org.uk. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/statement-intention-to-fine-marriott-international-inc-more-than-99-million-under-gdpr-for-data-breach/

ICO. (2020). *ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure*. ico.org.uk. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-marriott-international-inc-184million-for-failing-to-keep-customers-personal-data-secure/

ISO. (2018). *ISO/IEC 27000:2018(en) Information technology — Security techniques — Information security management systems — Overview and vocabulary*. iso.org. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en:term:3.54

ITGovernance. (2019). The 8 CISSP domains explained. *itgovernance.co.uk*. https://www.itgovernance.co.uk/blog/the-8-cissp-domains-explained#security-and-risk-management

ITRC & Cyberscout. (2017). Annual data breach year-end review. *Technical report, Identity Theft Resource Center*.

ITU. (2009). *Overview of Cybersecurity*. Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU). http://www.itu.int/rec/T-REC-X.1205-200804-I/en

Jensen, E. T., & Watts, S. (2017). A cyber duty of due diligence: Gentle civilizer or crude destabilizer? *Texas Law Review*, *95*(7), 1555-1577. https://search.proquest.com/scholarly-journals/cyber-duty-due-diligence-gentle-civilizer-crude/docview/1968929157/se-2?accountid=12870

Juchems, R. N. (n.d.). Enough is enough: 2018 has seen 600 too many data breaches. *Axel.org.* https://medium.com/@AxelUnlimited/enough-is-enough-2018-has-seen-600-too-many-data-breaches-9e3e5cd8ff78

Kemmerer, R. A. (2003). Cybersecurity. *Proceedings of the 25th IEEE International Conference on Software Engineering*, 705-715.

Lai, K. (2019, Feb 27). Dealmakers Struggle with Tech M&A due Diligence. *International Financial Law Review*. https://search.proquest.com/docview/2200496187?accountid=12870

Lewis, J. A. (2006). Cybersecurity and Critical Infrastructure Protection. *Center for Strategic and International Studies, Washington, DC*.

Lincoln, Y. S., & Guba, E. G. (1985). Establishing trustworthiness. Naturalistic inquiry. 289-331.

Mok, S. (2020, Jul 03). Protecting Personal Information in M&A Transactions. *China Law & Practice*. https://search.proquest.com/docview/2419772250?accountid=12870

Nash, K. S., & Minaya, E. (2018). Due Diligence on Cybersecurity Becomes Bigger Factor in M&A; Close scrutiny of tech operations can uncover cybersecurity gaps before deals close. *WSJ Pro. Cyber Security, New York*.

Nobel Media AB. (2020). *George A. Akerlof Facts*. Nobelprize.org. https://www.nobelprize.org/prizes/economic-sciences/2001/akerlof/facts/?fbclid=IwAR0MorMeWI02tPLzG6vYX5sqIzV59ngNjDfnjS5k7f7pp_Oq7ScqqdVkd6A

Oxford University Press. (2014, October 1). Oxford Online Dictionary. *Oxford: Oxford University Press*. http://www.oxforddictionaries.com/definition/english/Cybersecurity

Perry, & Herd. (2004). Reducing M&A risk through improved due diligence. https://www.emerald.com/insight/content/doi/10.1108/10878570410525089/full/html

Ponemon Institute. (2019). IBM: Cost of a Data Breach Report 2019. *Computer Fraud & Security*, *8 (2019)*(4).

Public Safety Canada. (2014). Terminology Bulletin 281:Emergency Management Vocabulary. *Ottawa: Translation Bureau, Government of Canada*.

Ragin, C. C. (1993). *Introduction to qualitative comparative analysis.* Cambridge University Press.

Rosenbloom, A. (2002). Due Diligence for Global Deal Making. *Bloomberg Press*. https://www.akademika.no/due-diligence-global-deal-making/9781576600924

Rouse, M., & Wigmore, I. (n.d.). Definition: Security incident. *Search Security*. https: //whatis.techtarget.com/definition/security-incident.

Shaban, H. (2017, June 13). It's official: Verizon finally buys Yahoo. *The Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2017/06/13/its-official-verizon-finally-buys-yahoo/?fbclid=IwAR0rsh_5_yE-YSZGvUy6IvVloXnrTYbF8020UN-aqwRP87bBXSpDZUxIhcs

Shaikh. (2018). Stock price value: Using event study analysis on the effect of information security incidents to your advantage. *Master's thesis in Information Security*, (NTNU).

Sherer, J. A., Hoffman, T. M., & Ortiz, E. E. (2015). Merger and Acquisition due diligence: A Proposed Framework to Incorporate Data Privacy, Information Security, E-Discovery, and Information Governance into due diligence Practices. *Rich. J.L. & Tech 5*, *21*(2). http://scholarship.richmond.edu/jolt/vol21/iss2/3

Shifter. (n.d.). *Derfor griper konkurransetilsynet inn mot Schibsted og Nettbil.* shifter.no. https://shifter.no/nyheter/derfor-griper-konkurransetilsynet-inn-mot-schibsted-og-nettbil/196003t

Shonka, D., & Rotert, M. (2020). Cybersecurity & due diligence: Avoiding liability for someone else's mistakes. *Property & Casualty 360*, *New York*.

The Software Engineering Institute (SEI). (2008). The Capability Maturity Model Integration.

Stopford, B., Wallace, K., & Allspaw, J. (2017). Technical Debt: Challenges and Perspectives. *IEEE Software*, *34*(4), 79-81. https://doi.org/10.1109/MS.2017.99

Storebrand. (n.d.). Storebrand. Retrieved November 09, 2020, from www.storebrand.no

Storebrand. (n.d.). *Security and Privacy*. Storebrand. Retrieved November 07, 2020, from https://www.storebrand.no/en/security-and-privacy

Storebrand. (2015). *Annual Report 2014*. Annual Reports. Retrieved 11 29, 2020, from https://www.storebrand.no/en/investor-relations/annual-reports/_/attachment/inline/0b895bcd-d12c-4311-bbf9-8aef4a541d46:493a217e3857e14b13d8bbfc718a1c9130fcd0b4/2014-annual-report-storebrand-asa.pdf

Storebrand. (2016). *Annual Report 2015*. Annual Reports. Retrieved 11 29, 2020, from https://www.storebrand.no/en/investor-relations/annual-reports/_/attachment/inline/d19cbaaf-381e-49f7-bacb-4d21502cc6d2:4da1e3a317843dc3c13d4c92a7db1c17572a270b/2015-annual-report-storebrand-asa.pdf

Storebrand. (2017). *Annual Report 2016*. Annual Reports. Retrieved 11 29, 2020, from https://www.storebrand.no/en/investor-relations/annual-reports/_/attachment/inline/dd49be26-1aee-4644-800d-61d367c17a65:fbd5960b90fdd03c0bfad2ddbf41fe62362850c7/2016-annual-report-storebrand-asa.pdf

Storebrand. (2018). *Annual Report 2017*. Annual Report. Retrieved 11 29, 2018, from https://www.storebrand.no/en/investor-relations/annual-reports/_/attachment/inline/aad74387-53a0-49de-9d39-fccd5ea48750:c25c0448e1a70ee3da07d5958d08e30d97d18631/2017-annual-report-storebrand-asa.pdf

Storebrand. (2019). *Investing in a sustainable future*. Annual Report 2018. Retrieved 11 29, 2020, from https://www.storebrand.no/en/investor-relations/annual-reports/_/attachment/inline/9e836443-a7b9-4375-aa8d-44bc88e809dc:e34f5b7e1bd5cde11fec7aa470e1930229c4692e/2018-annual-report-storebrand-asa.pdf

Storebrand. (2020). *Annual Report 2019*. Storebrand – Annual reports. Retrieved 11 29, 2020, from https://www.storebrand.no/en/investor-relations/annual-reports/_/attachment/inline/d0e9764c-1757-4fe1-a96b-c71c90a998a4:7cf55a6b7cc6fcd106f6bad885985c4c3608b11d/2019-annual-report-storebrand-asa.pdf

Stretton, H. (1969). The Political Sciences: the General Principles of Selection in Social Science and History. *American Political Science Review*, *63*(3), 944 - 945. https://doi.org/10.1017/S0003055400258863

Teece, D. J. (2018). Profiting from innovation in the digital economy: Enabling technologies, standards, and licensing models in the wireless world. *Research Policy*, *47*(8), 1367-1387.

Visma. (n.d.). *Visma*. Visma. Retrieved November 11, 2020, from www.visma.com

Visma. (2015). *Annual Report 2014*. Financial Reports Visma. Retrieved 11 29, 2020, from https://www.visma.com/globalassets/global/visma.com/annual_reports/visma_annual_report_2014.pdf

Visma. (2016). *Annual Report 2015*. Financial Reports Visma. Retrieved 11 29, 2020, from https://www.visma.com/globalassets/global/visma.com/annual_reports/visma-annual-report-2015.pdf

Visma. (2018). *Annual Report 2017*. Financial Reports Visma. Retrieved 11 29, 2020, from https://www.visma.com/globalassets/global/common-images/documents/visma-annual-report-2017-dbl.pdf

Visma. (2019). *Annual Report 2018*. Financial Reports Visma. Retrieved 11 29, 2020, from https://www.visma.com/globalassets/global/visma.com/annual_reports/annual_report_2018-2.pdf

Visma. (2020). *Annual Report 2016*. Financial Reports Visma. Retrieved 11 29, 2020, from https://www.visma.com/globalassets/global/visma.com/annual_reports/visma-annual-report-2016.pdf

Visma. (2020). *Annual Report 2019*. Financial Reports Visma. Retrieved 11 29, 2020, from https://www.visma.com/globalassets/global/visma.com/annual_reports/visma_2019_annual_report_final.pdf

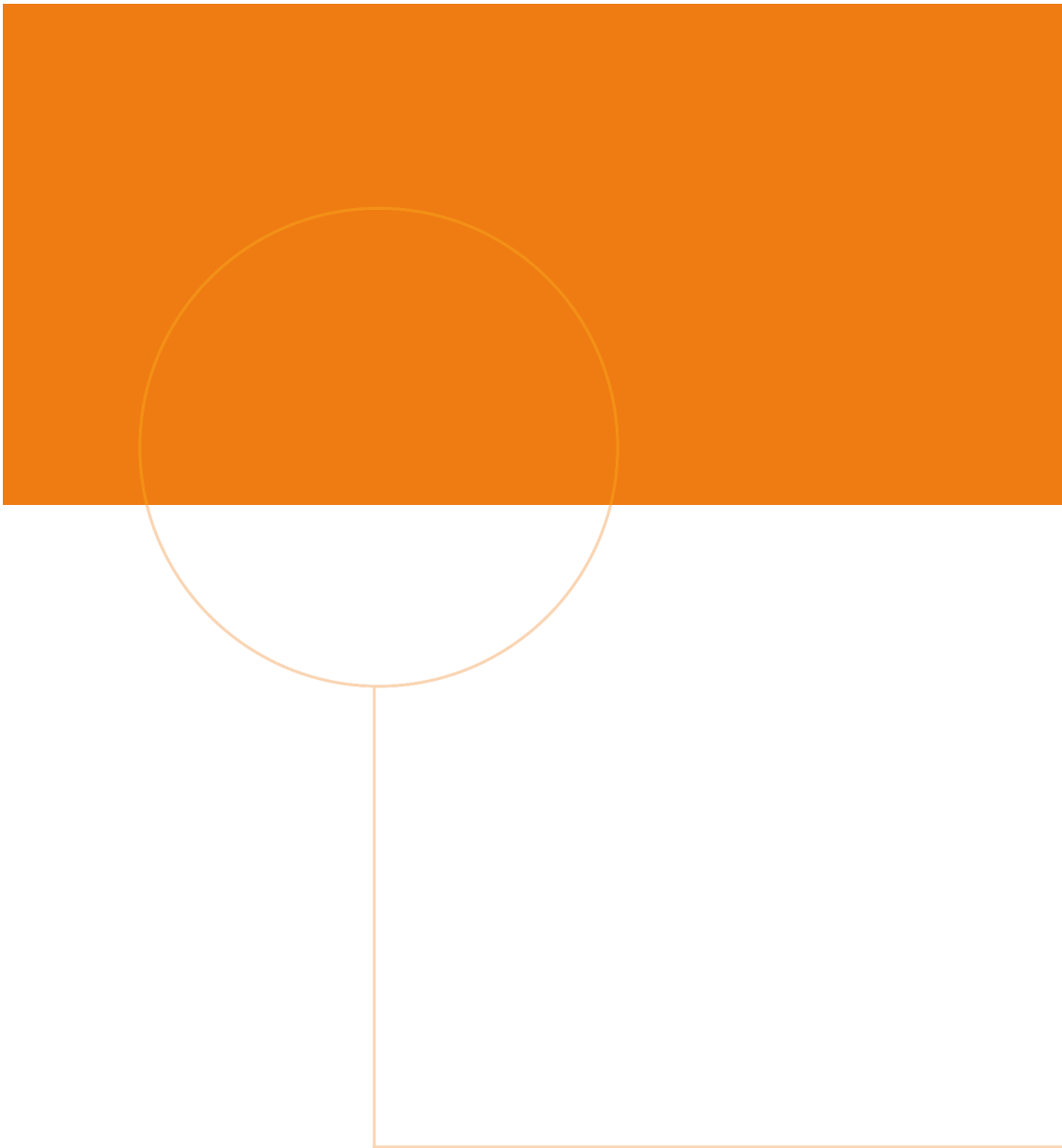
Welgan, J. (2016). Cybersecurity concerns in M&A due diligence. *Risk Management*, *63*(9), 10-11. https://www.proquest.com/scholarly-journals/cybersecurity-concerns-m-amp-due-diligence/docview/1845753926/se-2?accountid=12870

World Economic Forum. (2020). The Global Risks Report 2020. *Insight Report*. http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf?fbclid=IwAR0MorMeWI02tPLzG6vYX5sqIzV59ngNjDfnjS5k7f7pp_Oq7ScqqdVkd6A

Yin, R. K. (2013). Validity and generalization in future case study evaluations. *Evaluation*, *19*(3), 321-332.

Yin, R. K. (2015). *Qualitative research from start to finish*. Guilford Publications.

Yin, R. K. (2017). *Case study research and applications: Design and methods.* Sage publications.



NTNU
Norwegian University of
Science and Technology

NTNU SCHOOL *of*
ENTREPRENEURSHIP