



Information Security in Mergers and Acquisitions

Harri Hautala

Master's thesis

05 2024

Master's Degree Programme in Information Technology, Cyber Security

Hautala, Harri

Information Security in Mergers and Acquisitions

Jyväskylä: JAMK University of Applied Sciences, May 2024, 77 pages

Master's Degree Programme in Information Technology (Cyber Security). Master's thesis.

Permission for open-access publication: Yes

Language of publication: English

Abstract

Mergers and Acquisitions (M&A) provide companies with the possibility of inorganic growth. Many companies have most of their information assets in digital form. Therefore, ICT integration is a vital part of a merger. Both M&A and ICT integration are widely researched subjects. However, the increasingly important information security has lacked research inside this context until this thesis was written.

The research aimed to investigate the role of information security in mergers and acquisitions. The aim was to identify the role of the information security specialists in the process and how they would improve it. A systematic literature review and expert interviews with information security professionals provided the foundation for this study.

The research used qualitative methods, focusing on thematic interviews with high-level information security specialists. It combined literature reviews and interviews to form a comprehensive analysis and a synthesis model.

The study highlighted the importance of integrating information security into M&A processes to ensure better alignment with business goals and to mitigate potential risks. The findings suggest that systematic and proactive information security measures can mitigate potential risks. Future research should focus on quantitative analysis of the early integration of information security measures into the M&A process and the testing of the effectiveness of the Information Security Alignment Model.

Keywords/tags (subjects)

Mergers and acquisitions, information security, product security, due diligence, CISO, residual risk, procurement risk, information security alignment model

Yritysfuusiot ja yritysostot (M&A) tarjoavat yrityksille mahdollisuuden epäorgaaniseen kasvuun. Useimmilla yrityksillä on suurin osa tietovaroistaan digitaalisessa muodossa. Siksi ICT-integraatio on tärkeä osa fuusiota. Sekä yritysjärjestelyt että ICT-integraatio ovat laajasti tutkittuja aiheita. Yhä tärkeämpää tietoturvaa ei kuitenkaan ole juurikaan tutkittu tämän kontekstin sisällä ennen tätä opinnäytetyötä.

Tutkimuksen tavoitteena on selvittää tietoturvan roolia fuusioissa ja yrityskaupoissa. Tavoitteena on tutkia, miten tietoturva-asiantuntijat osallistetaan prosessiin ja miten he parantaisivat sitä. Järjestelmällinen kirjallisuuskatsaus ja teemahaastattelut kokeneiden tietoturva-ammattilaisten näkemyksistä antavat pohjan tälle tutkimukselle.

Tutkimus on toteutettu laadullisena tutkimuksena keskittyen kokeneiden tietoturvajohtajien teemahaastatteluihin. Tutkimuksessa yhdistetään kirjallisuuskatsaus ja teemahaastattelut kattavaksi analyysiksi ja synteesimalliksi.

Tutkimustuloksissa korostuu tietoturvan integroinnin tärkeys yrityskauppaprosesseissa, jotta sitä kautta voidaan varmistaa parempi yhteensopivuus liiketoiminnan tavoitteiden kanssa ja vähentää mahdollisia riskejä. Tulokset viittaavat siihen, että järjestelmälliset ja ennakoivat toimenpiteet tietoturvan huomioimiseksi voivat pienentää mahdollisia riskejä. Tulevaisuuden jatkotutkimuksessa tulisi keskittyä tietoturvatoimenpiteiden varhaisen integroinnin kvantitatiiviseen analysointiin, M&A-prosessiin ja liiketoiminnan tietoturvamallin luotettavuuden testaamiseen.

Keywords/tags (subjects)

yrityskaupat, sopimusriski, tietoturvan arviointi, tietoturvan strategiamalli

Miscellaneous (Confidential information)

Null

.

Contents

1	Introduction	5
1.1	Motivation for the study	5
1.2	Aim of the research	6
1.3	Acronyms.....	7
1.4	Thesis structure	8
2	Research Design, Methods and Data	9
2.1	Research Design and Strategy	9
2.2	Methodology.....	9
2.2.1	Reliability, Validity and generalization	10
2.2.2	Ethics.....	11
2.3	Previous research	12
2.4	Literature review process.....	13
2.5	Methodology for literature review	14
	Information sources used for literature review	14
2.6	Data collection and access to data.....	15
2.6.1	Limitations of the data.....	15
2.6.2	Interview as part of data collection	15
3	Research process: How this research was conducted.....	16
3.1	Information sources	16
3.2	Data Collection Process.....	17
3.3	Discussion Topics for the Interview	17
3.4	Methods to Analyze the Data	18
4	Theory.....	19
4.1	Mergers and Acquisitions.....	19
4.1.1	Types of M&A	20
4.1.2	M&A Process.....	21
4.1.3	Due Diligence as Part of M&A	22
4.1.4	Cyber Due Diligence with Due Diligence	23
4.2	Role of Information security and ICT in M&A	25
4.2.1	Merging ICT Systems.....	25
4.2.2	Post-merger ICT integration levels	27
4.2.3	Information Security inheriting risk blindly in M&A.....	28
4.3	Strategy and Information Security	29
4.3.1	Relation between ICT functions, management and strategy of an organization..	29

4.3.2	Relation between digital security and strategy of an organization	30
4.3.3	Information Security Policy, Information Security Management systems and Strategy 32	
4.3.4	Information security skills in company board and the role of CISO	33
4.4	Designing product and service offerings for cybersecurity from the start.....	34
4.5	M&A Risks	35
4.5.1	Points of Failure in M&A.....	36
5	Results from the interviews	36
5.1	Overview	36
5.2	Due Diligence process.	38
5.2.1	Technical Information Security Needs Improvement.....	39
5.2.2	Due Diligence to serve pre-integration planning	39
5.3	The topics of discussion when assessing target company's security.....	40
5.3.1	Preliminary questionnaire and meeting	40
5.3.2	Security policy and management	41
5.3.3	ICT policy.....	41
5.3.4	Incident management and public security footprint.....	41
5.3.5	Nature of Assessment Meetings.....	42
5.4	Product security vs organization security	42
5.5	Tight timeframe and urgency of the process.....	43
5.6	Business culture	44
5.7	Treating inherited system risk.....	44
5.7.1	Legacy systems and technology debt	44
5.7.2	Procurement risk	45
5.7.3	Asset management	46
5.7.4	Residual Risk Treatment	46
5.7.5	Unintentional error.....	47
5.8	Paper Tigers.....	47
5.9	M&A Activity Activates Criminal Actors.....	48
5.10	CISO and information security organization involvement	48
5.10.1	Stage A: Informed In Initial Deal Making	50
5.10.2	Stage B: Consulted In Initial Deal Making.....	50
5.10.3	Stage C: Consulted in Due Diligence	50
5.10.4	Stage D : Responsible in Due Diligence	50
5.10.5	Stage E: Responsible in Pre-integration planning.....	51
5.10.6	Stage F and G: Responsible or Accountable in integration	51

5.11	The relevance of information risk to the deal	51
5.12	Identity and Access Management.....	52
5.13	Industry-Specific or General Regulations.....	52
5.14	ICT Integration.....	53
5.15	Key-persons leaving the Company	54
5.16	Infosec Communication Skills.....	55
6	Discussion and conclusions	56
6.1	Limitations of evidence	57
6.2	Discussion	58
6.2.1	Interpretation And Synthesis Of Results	61
6.2.2	Ethical And Quality Discussion.....	64
6.3	Conclusion	65
7	Acknowledgment.....	65
	References	67
	Appendix 1. Interview Discussion Topics.....	71
	Appedix 2. RACI matrix.....	73

Figures

Figure 1: Focus of this research indicated with red colour.....	12
Figure 2 classification of post-merger integration levels	27
Figure 3: Four Elements of Organizational Resilience to Cyberattack.....	31
Figure 4: View from the Quircos screen capture demonstrating the subjects that raised in the interviews.....	37
Figure 5: The four stages of M&A activity - and the extend to which CISOs are involved	48
Figure 6: The four stages of M&A activity and CISO role -results of the interviews	49
Figure 7: Information security alignment model.	62

1 Introduction

1.1 Motivation for the study

The idea for this topic came from a recent discussion in a hacker discussion group. In the discussion, I suggested making a thesis on this topic. The response was very positive, and I was strongly encouraged to continue the work. I also received contact information from several people willing to give an interview or discuss their experiences in mergers and acquisitions. The thesis topic also touches on my work duties, as my employer's board of directors decided to divest the Finnish operations. I intend to gather information on the topic from different industries and actors of different sizes to gain perspective and develop essential skills in my work.

The aim is to determine information security's role in acquisitions and the related due diligence process. The process is challenging from a security perspective, as the company's confidential information ends up in the hands of many consultants and the acquiring party. One aspect of the work is to consider how to harden and improve the security of the process. Another topic to consider is administrative security in the due diligence process. Organizations have very different ways to organize and perform information security activities, so these often must be coordinated carefully in business acquisition. One hypothesis is that in the acquisition process, the target company should be seen as similar to any other company in the supply chain, but with the difference that the security assessment is iteratively taken further than in a normal supply chain assessment process.

Mergers and acquisitions are strategic tools used by companies seeking rapid growth and expansion into new markets or to acquire additional workforce. However, the success of these ventures often hinges on the compatibility and integration of information technology systems between the entities involved. Studies, including one from Harvard Business Review, suggest that 70-90% of M&A deals fail due to various reasons, with IT incompatibility being a significant factor (Tervola, 2023).

Today every merger and acquisition brings many potential digital risks with it. From small to large, simple to complex, all M&A deals involving technology have cybersecurity challenges (Rosenquist, 2020).

1.2 Aim of the research

This paper discusses how information security is handled in corporate M&A:s. More precisely, the aim is to find answers to these research questions:

- How are CISOs involved in the M&A process? The literature review reveals that CISOs are often invited to participate in a very late phase of the M&A process. What if the CISO had been involved earlier?
- How is information security considered in the ICT integration process? The literature review discusses that information security analysis should be part of the Due Diligence process.
- How much does DD include information security? What is the appropriate level?

Company processes are often heavily dependent on ICT infrastructure and systems. The literature review also revealed that Due Diligence should involve information security.

1.3 Acronyms

Acronym	Explanation
CIO	Chief Information Officer.
CISO	Chief Information Security Officer
CMDB	Configuration Management Database. A database for storing information on hardware and software assets.
DD	Due Diligence
GDPR	General Data Protection Regulation
IAM	Identity and Access Management. A systematic approach to manage user rights
IPR	Intellectual Property Rights. Legal rights to the use of intellectual creations
ISF	Information Security Forum
M&A	Mergers and Acquisitions
NIST	National Institute of Standards and Technology
PDCA	Plan Do Check Act
SME	Small or Medium size Entrepreneurship
SIEM	Security Information and Event Management

1.4 Thesis structure

The thesis consists of a literature review, research design and methods.

Research Design and Methods.

This section of the master's thesis outlines the methodological approach to investigating the research questions. The approach is to investigate the subject with qualitative research methods. An important part is to evaluate the reliability, validity, and ethical considerations.

Research Process

The research process section explains the practical steps taken to conduct the research. The information sources were ten Finnish information security experts working as CISOs or equivalent high-level information security positions and having hands-on experiences from one or more M&A processes. The reasoning for the methods used and topics discussed is also explained.

Theory

The theory section includes a literature review that presents the current research covering M&A, ICT integration, information security, and risk. M&A is a widely researched and popular subject in business research. There are also plenty of magazine and journal articles covering the subject.

Another part of the literature review discusses ICT's role in M&A. Although there is a significant difference between information security and ICT, there are also overlapping items in technology, so the role of ICT needs to be covered.

The third part of literature review covers the strategic level of information security. This part is a combination of strategic literature and information security literature to highlight the strategic role of information and through that also information security.

Results From Interviews

This section focuses on the findings from interviews and opens the understanding of the real-world implications of information security practices in M&A context. The structure follows the

topics of discussion in the interviews. The findings are the synthesis of the discussions added with direct quotations (although translated from Finnish to English) from the interviewees. The interviewee's names or company names are not revealed.

Discussion and Conclusions.

The concluding section summarizes the research questions and the answers found in the research material collected through interviews. This section also lists the new findings that the researcher made based on the interviews. This study has its limitations, and they are discussed here too to make sure the reader will not make wrong interpretations from this study.

2 Research Design, Methods and Data

2.1 Research Design and Strategy

The aim of this study is to investigate the role of information security in mergers and acquisitions (M&A), as well as in related ICT integration projects. First, a systematic literature review is conducted, which examines publications to clarify the subject areas. Second, the research utilizes the views of reliable IT experts and other experts through interviews. The goal is to identify information security-related success factors and possible shortcomings that affect the outcome of M&A projects. The research strategy consists of literature reviews, case studies and interviews, which form a comprehensive analysis.

The aim is to reach people's own descriptions of their perceived reality. These descriptions are assumed to include those things that a person considers meaningful and important in their life (Vilkka, 2019).

2.2 Methodology

Perhaps the worst mistake a researcher can make is collecting and describing data without a clear interpretation. Descriptive research can produce new information, but if this new information is not parsed into a part subject, its value remains contingent. The hallmark of research is that it leads to a clear conclusion to an interpretation that can be discussed earlier with research. In the

end, interpretation is the distinguishing feature about the everyday order of research. A clear interpretation is also easy to communicate to the public (Koskinen et al., 2005).

2.2.1 Reliability, Validity and generalization

Validity is understood as the extent to which a certain statement, interpretation or result expresses the object to which they are intended to refer. Types of validity are considered to be minimally internal and external validity. Internal validity means the internal logic and consistency of the interpretation. External validity, on the other hand, means whether the interpretation generalizes to others than to the investigated cases (Koskinen et al., 2005).

Qualitative researchers should be careful not to claim that their results are generalizable if the claim is clearly contradictory with statistical thinking (Koskinen et al., 2005).

Koskinen et al. (2005) discuss the problematic nature of generalization in qualitative research. Qualitative data is usually a purposefully selected sample, not a sample collected by randomization. There are several reasons for the low number of cases, Qualitative research is most often carried out to collect a relatively large amount of data from a small number of cases.

If reliability and validity thinking is taken seriously, the sources of error contained in the research should be systematically evaluated at the end of the study. These sources of error should be considered when designing the study. They should be anticipated and minimized. In fact, an essential part of a researcher's professional skills is precisely the ability to locate sources of error and control them (Koskinen et al., 2005).

Internal validity in this research

The goal is to find possible information security perspectives for much-researched subject areas in business economics and computer science. These points of view cannot be generalised unless statistically reliable follow-up research is carried out. The information security perspective is under-researched in otherwise widely researched subjects, mergers and acquisitions.

External validity in this research

The larger sample of corresponding experts in the ISF report has given a similar result. That survey's sample is larger, so it is statistically more reliable than this research. In this research, the significance lies in the search for the underlying explanations and justifications rather than a reliably consistent sample. There is an obvious need for further research to find statistically solid evidence for these explanations and justifications.

2.2.2 Ethics

The JAMK ethical principles of research have been considered in every phase of the research process.

Privacy and secrecy are to be considered throughout the research process. The confidentiality of the information is a big challenge because the interviewees are bound by various non-disclosure agreements. As a result, they cannot naturally talk about any data security breaches they may have experienced. It would also be questionable in terms of research ethics to reveal confidential information intentionally or unintentionally. For this reason, it is necessary to ensure that the layout of the questions is correct and explicitly emphasize to the interviewees that the intention is not to steal confidential information under any circumstances.

If it is assumed that the research subjects do not know how to assess the risks that the research may pose to them, it is the researcher's task to inform them of the possible risks the research entails and what means are used to anticipate these harms. Such a procedure is called "informed consent" (Koskinen et al., 2005).

Ethical procedures and procedures aimed at arousing confidentiality shall be communicated at different stages of the investigation. At the beginning of the research, the researcher has to explain a variety of things, such as the reasons and background of the research, their own motives, questions related to how the research is conducted and the ethical principles followed (Koskinen et al., 2005).

2.3 Previous research

There is very little research on this research topic. The only approach is to try to find links from research that discusses M&A, due diligence process, ICT integration and migration projects, Information security breaches and supply chain security.

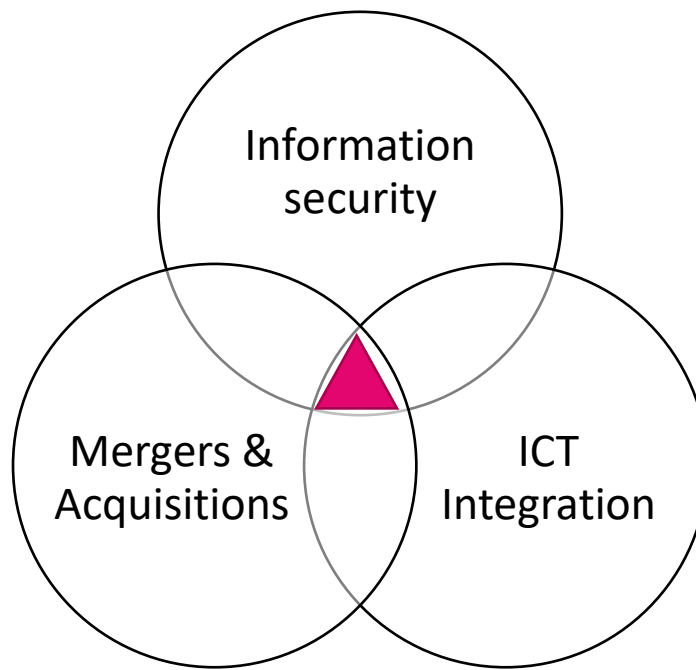


Figure 1: Focus of this research indicated with red colour

According to figure 1, the research area is at the intersection of information security, ict integration and the M&A process.

Research on Mergers & Acquisitions

Business sciences have studied mergers and acquisitions for decades. There is a lot of research available. Looking at the publishing dates of the research, there is a trend that the research is done in cycles. Reading the research papers, it appears that the more M&As occur, the more research is done afterwards.

Research on ICT Integration

Business information is mainly stored in digital form and protected with different means of ICT security. ICT systems have grown more complex over the years, covering a wider range of business processes. When integrating two organizations' ICT systems, there is an increased risk level

because the systems have different histories, and the reasons they have been built in a certain way differ. This complexity and the backgrounds have been a research subject. The most visible risks are delays in implementation, identity and access management, or other usability-related risks. Perhaps, therefore, these are the most typical research subjects, too, leaving information security in the shadows.

2.4 Literature review process

PRISMA 2020 flow diagram for new systematic reviews which included searches of databases, registers and other sources

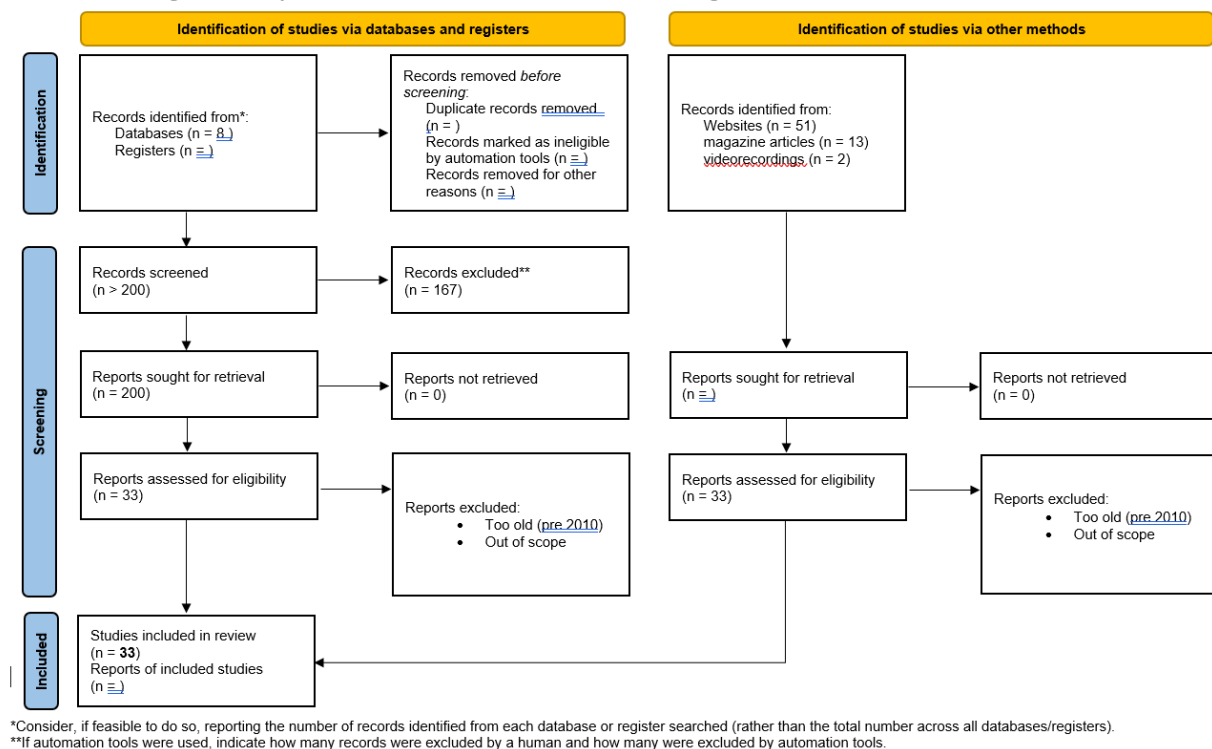


Figure 1: Literature review process.

The literature review process started by searching and identifying academic papers from some eight relevant databases. The result was slightly less than 200 records from the searches, of which some 167 records were excluded, and 33 records of academic papers were used. Figure 1 demonstrates the process with Prisma flow diagram standard (*PRISMA 2020 Flow Diagram*, 2024).

Some records were excluded because the research paper was out of scope for some reason or was too old with research findings tightly linked to outdated technology or equivalent reasons.

2.5 Methodology for literature review

Information sources used for literature review

The following online-databases and portals has been used as sources for references:

Database	Link
ACM Digital Library	https://dl.acm.org/
ResearchGate	https://www.researchgate.net/
Turvallisuus ja riskienhallinta	https://www.lehtiluukku.fi/lehdet/turvallisuus_riskienhallinta/
Harward Business Review	https://hbr.org/
MIT Sloan Management Review	https://sloanreview.mit.edu/
Janet Finna	https://janet.finna.fi/MyResearch/Favorites
Theseus	https://www.theseus.fi/
O'reilly.com	https://learning.oreilly.com/

Search strategy and selection process for information sources

The used search words and phrases are listed below:

- information security in M&A
- Information security due diligence
- due diligence process
- cyber security due diligence
- CISO role
- Information technology in mergers and acquisitions
- ICT integration

Research that is over 10 years old needs to be treated more critically. Information security, and especially cyber security, has evolved significantly in ten years. The threat landscape has changed, and many new technologies such as cloud computing have been introduced and applied on a wide scale during these years.

2.6 Data collection and access to data

This research is qualitative research and information gathering is performed through interviewing information security experts who have solid experience of M&A activities.

2.6.1 Limitations of the data

The time spent collecting data is often short. This does not preclude the use of participatory observation. More important than the time spent is the appropriate delimitation of the research problem and questions and the research objectives in relation to the chosen methods (Vilkka, 2019).

2.6.2 Interview as part of data collection

The thematic interview is based on key themes selected in advance and related clarifying questions. The advantage of a themed interview is that the questions can be specified and deepened during the interview based on the answers of the interviewees. Methodologically, the theme interview highlights how individuals interpret and assign meanings to things and how these meanings are constructed through interaction.

The interview is chosen as the research material, in which people's experiences are collected through oral communication. The research data collected through a thematic interview can be converted into the form required for statistical analysis and into quantitative research. Thematic interviews and open-ended questions are used in the research method when there is little information about the matter or phenomenon being studied (Vilkka, 2019).

Koskinen, Alasuutari, and Peltonen (2005) state that structured interviews usually refer to a survey interview in which the researcher determines the questions and the order in which they are asked and usually also gives the answer options. A semi-structured interview, also called a thematic interview in Finland, allows the interviewee more freedom. The researcher prescribes the questions, but the interviewee can answer them in his own words and sometimes even suggest new questions. The interviewee may also deviate from the order of the questions. Semi-structured

interviews should be distinguished from in-depth interviews, which aim to minimize the researcher's influence on the interview situation. At its purest, an in-depth interview is structured so that the researcher mainly has a general interest that he or she wants to discuss with the interviewee. The interviewee answers in their own words and ultimately defines the questions as reflecting their thinking.

A structured interview aims to get meaningful responses that align with the research's objectives and the problem statement or research task. Typically, the predefined themes are based on the research's reference framework, encompassing existing knowledge about the studied phenomenon. However, depending on the openness of the thematic interview, the relationship between the questions contained in the themes and those presented in the reference framework of the study varies from allowing intuitive and experiential observations quite strictly to only sticking to questions that are known in advance (Tuomi & Sarajärvi, 2019).

3 Research process: How this research was conducted

3.1 Information sources

The research is conducted by selecting ten information security officers (CISO) who have a long track record (at least five years of experience) in information security manager roles and also experience in more than one M&A process. There are no geographical limitations to the invitation, but all the persons interviewed are Finnish. The invitation was sent to LinkedIn and to a closed Finnish infosec forum.

Number of Interviewees

Qualitative research does not aim for statistical generalizations. Instead, qualitative research aims, e.g., to describe some phenomenon or event, to understand a certain activity, or to give a theoretically meaningful interpretation of something related to the phenomenon. Thus, according to principles in qualitative research, it is important that the persons from whom the information is collected, preferably know about the research subject as much as possible or have experience with the matter. In this sense, the choice of informants should not be random but should be considered and fit for the purpose (Tuomi & Sarajärvi, 2019).

The interviewees were carefully chosen from the volunteers mentioned above. Their backgrounds were confirmed and recorded at the beginning of each interview session.

3.2 Data Collection Process

The interviews were conducted in a Microsoft Teams meeting, which was recorded and transcribed. For security and data retention, the JAMK M365 student instance was used since it will be erased when the study time is over. Video recordings and transcriptions are confidential, and when referred to an interview, the interviewed person's name is replaced by a letter.

Reliability and Validity in the Interviews

The discussion topics were chosen based on the literature review. The topic validity was also tested by asking the interviewees at the beginning of each discussion topic if this topic was valid. Also, they were asked to express clearly what should be discussed in addition to these topics. This way the coverage of topics was validated.

3.3 Discussion Topics for the Interview

According to Tuomi & Sarajärvi (2019) the aim of the thematic interview is to find meaningful answers in accordance with the purpose of the research and the problem statement or research task. The themes chosen are based on the research questions.

There were altogether six topics of discussion prepared for the interviews. Each topic had some questions generated from the literature review. The interviewees were guided to talk freely of the topic and asked to be critical towards the leading questions within each topic. The general guidance was that the interviewee can freely express at any time if there is a vital point missing from the topic, or if the questions were irrelevant. This way the interviewees were not limited to the discussion topics.

The Discussion Topics

There were in total six topics of discussion:

1. Interviewee's background
2. Due diligence process
3. Treating inherited system risk
4. ICT Integration
5. Side effects of M&A process
6. Risk scenarios

3.4 Methods to Analyze the Data

The transcriptions are exported to Qircos (a software tool designed for processing qualitative research) for categorizing the data. The categorizing process helped in raising key aspects that were discussed across all interviews.

The transcriptions needed proofreading because the automated transcription in Microsoft Teams interpreted the speech a bit wrong. Therefore, the first round of reading was proofreading at the same time.

In addition to transcriptions the researcher's handwritten notes were also transferred to electronic form and added to the transcriptions.

All these documents were imported to Quircos for the analysis. All relevant items were labelled in the software, and labels were added when new items when something relevant appeared from the transcription. There were several items that the interviewees explicitly stated to be important. Some items were expressed as questions within the discussion topics but there were several items that appeared only when analyzing the interview materials. Communication skills, IAM, company culture, are examples of such topics.

4 Theory

4.1 Mergers and Acquisitions

The term Mergers and Acquisitions (later referred to as M&A too) is the term that describes a very wide area of financial activities where two or more organizations change their ownership relations. Here are some definitions found in literature that explain - but not exclusively - the meaning of the term Mergers and Acquisitions. Academic studies over the years covering M&A have been criticized for their inability to provide “robust” theories to explain the dynamics and value-creation mechanisms of a merger or an acquisition (Junni & Teerikangas, 2019).

In other words, a merger is the combination of two or more companies, where the acquiring firm takes on the assets and liabilities of the acquired company or companies. Despite the significant changes caused by the merger, the buying company typically retains its original identity. (Sherman, 2018)

Acquisition is the purchase of an asset such as a plant, a division, or even an entire company (Sherman, 2018).

Sherman (2018) states that the distinction between merger and acquisition both result in the same outcome. Two or more companies that had separate ownership and operations end up under the same roof usually to obtain some strategic or financial objective. Acquisition typically refers to cases where one company is the buyer, and another company is the seller.

Companies’ top management considers mergers and acquisitions to be strategic growth opportunities. However, a large body of evidence suggests that there is a significant variance in the returns from M&A (Benitez et al., 2018).

The role of ICT has not received adequate attention or has not been understood. One well-known example from the USA is Wells Fargo’s acquisition of First Interstate, which suffered from significant problems in customer database integrations between the two banks, causing considerable negative effects in customer service levels, leading to significant loss of customers, decreasing Wells Fargo’s ability to realize the full value of the acquisition. (Benitez et al., 2018)

Yahoo is another sample case where a large-scale breach caused a significant impact on an M&A deal with Verizon. Reuters news from Feb 21, 2017, reveal the case:

“Verizon Communications Inc announced it will acquire Yahoo Inc's core business for \$4.48 billion, a reduction by \$350 million due to two major cyber-attacks on the internet company. The deal, initially announced seven months before in July, had been delayed as the companies assessed the damages from the two data breaches Yahoo disclosed last year. The leading U.S. wireless carrier had been attempting to convince Yahoo to modify the terms of the agreement because of the cyber-attacks”. (Athavaley & Shepardson, 2017)

All three components of the security CIA triad are jeopardized in Mergers and Acquisitions, since the process includes significant amounts of data sharing and data integration. Security measures must assess risks in a wide range of areas (Rosenquist, 2020).

4.1.1 Types of M&A

A company acquires another company to gain access to a new product line, customer segment, or geography. (Sherman, 2018). There are various other M&A types, each characterized by various features, motives, and challenges (Junni & Teerikangas, 2019). M&A motivation is to aim for synergies, typically economies of scale or scope. To achieve these synergies, companies must undergo some degree of integration of processes and information flows. The practical level brings ICT and information security to focus.

Gaughan (2017) categorizes mergers into three categories. A horizontal merger takes place when two competitors join forces to gain market share. Vertical mergers involve integration of companies with a buyer-seller relationship. In a conglomerate merger two or more companies from different industries merge, forming a portfolio of various sectors.

Gaughan (2017) states that Mergers may be paid for in several ways, typically cash, securities, or a combination of these two. Price is the most important issue, and beyond anything else, it defines the amount of value transferred to the seller in return for ownership of the business (Sherman, 2018).

4.1.2 M&A Process

M&A can optimize the capital structure of companies through transfer of ownership and property rights (Chui, 2011). Absalom (2022) describes that M&A deals largely follow a four-step process :

1. Initial deal-making
2. due diligence
3. Pre-integration planning
4. Integration

Chui (2011) proposes a risk management approach that manages and reduces the risks associated with M&A activities and eventually minimizes the failure of M&A. The risk management model is employed to identify and manage risks associated with M&A processes by dividing the process into two steps: risk identification and risk quantification.

BearingPoint's (2023) study shows that market extension has been the primary driver of M&A. Most respondents highlighted that Digital transformation has significantly influenced the M&A strategies of companies that made several acquisitions during 2018 -2023.

In more detail, 69% of the respondents said they considered digital transformation a crucial reason for acquisitions. 38% of the respondents said that access to digital delivery models has been a crucial driver in their M&A strategy. New technological solutions can increase their competitive advantage and enable them to scale their business. 31% of the interviewed companies mentioned scalability opportunities was a key factor in digitalization strategy (*M&A Integration and Carve-out Study*, 2023).

BearingPoint (2023) study raised some factors of successful M&A integration. First, the integration planning should begin before the closing of the deal. A clearly defined integration end-state target is considered one of the most important success factors. Additionally, the top management's support of adequate resourcing is also rated among the most important success factors for integration. Secondly, companies that complete multiple M&A integrations view a deep level of integration as the most desirable. Thirdly, alongside hard metrics, qualitative measures such as the

retention rate of acquired employees and customer satisfaction are essential. Lastly, the research suggests that companies with more experience with acquisitions put more emphasis on cultural factors already in the pre-closing phase.

4.1.3 Due Diligence as Part of M&A

Wright and Altamas (2015) define due diligence as follows: Due diligence involves auditing the potential investment to verify all essential facts and assumptions before entering into a contractual agreement with the other party involved. Typically formal, this process serves as the foundation for any subsequent contracts or agreements.

According to Wright & Altamas (2015) The growing reliance on IT and online platforms, coupled with the rise in cyber security threats and alterations in the development procedures for new systems, has underscored the importance of IT within these transactions. In the case of larger organizations or transactions, there is now an increased demand for IT consultants to provide guidance and support during due diligence assessments. Furthermore, IT is acknowledged as a critical element of any transaction, given that addressing IT-related issues post-acquisition can incur substantial expenses, which ideally should have been identified during due diligence. In some cases, it may be worth considering cancelling the deal immediately if the costs associated with resolving IT issues would make the deal too expensive (Wright & Altamas, 2015).

Wright & Altamas (2015) note that the primary focus of IT due diligence should align with that of any other financial due diligence, namely, assessing how the findings influence the proposed deal's feasibility, its overall viability, or its value.

4.1.4 Cyber Due Diligence with Due Diligence

Acquiring or merging with a company without analyzing its digital asset protection could be as risky as buying a company without studying its financial statements. (Farrell, 2014)

Farrell (2014) lists that the buyer should ask about target company's sensitive data, where data is stored and how data is protected from outsiders. The sensitive data should also be protected from internal leaks.

Grimberg & Ray (2018) describe the cyber due diligence process clearly: the process should start with identifying and listing the vulnerabilities and gaps in the target organisation's information security program. A good practice is to compare the existing program to commonly accepted guidelines and cyber security frameworks such as NIST or ISO 27001 as an example. The assessment should present a report for the stakeholders that consists of findings, rankings and prioritized list of recommendations.

Grimberg and Ray (2018) suggest that a cybersecurity assessment should start by collecting information and data. The team conducting the assessment should carry out comprehensive interviews with both internal and external ICT service providers, along with other crucial stakeholders, to establish a foundational understanding of the organization's existing cybersecurity program.

Wright and Altimas (2015) suggest having set of tasks in the due diligence process to assess essential ICT system's resilience and reliability:

- ICT strategy.
- The age and life cycle of the applications and supporting infrastructure.
- The service level agreements and life cycle of the external suppliers.
- Maintenance and unplanned downtime logs of the systems due to incidents and problems.
- System resilience strategy.
- ICT security.

Wright & Altimas (2015) suggest adopting a high-level perspective to evaluate if the systems are suitable for their intended use by considering:

- The business and regulatory requirements and the systems' compliance with these regulations.
- The systems' age and how often they fail.
- The strategy for upgrading and patching, and its suitability for the current context.
- The resilience strategy of the systems and its appropriateness for the industry.
- The IT security measures in place and their suitability for specific circumstances.

Given the high prevalence of information security breaches across various sectors, Wright and Altimas (2015) state that ICT security has become a key issue discussed in boardrooms, with chief executive officers (CEOs) and chief financial officers (CFOs) showing at least a basic understanding of its importance. Many organizations aim to get their information security management system (ISMS) certified under ISO27001 or other equivalent standards (Wright & Altimas, 2015).

Wright and Altimas (2015) place a relevant question: Is nation-state- hacking relevant to a due diligence project? It is comparable to leaving the doors to the research and development offices open to let anyone come in and steal the designs, reveal patents and copy them. This results in significant loss of intellectual property and subsequently declines the company's value. If such a breach is discovered during due diligence, the value of the target company reduces significantly (Wright & Altimas, 2015).

Wright and Altimas (2015) state that, when evaluating IT systems, technology should not be the sole consideration. They emphasize that three key components are highly relevant: process, people, and technology.

Sony incurred significant costs when its PlayStation network was down for several weeks and the group LulzSec accessed millions of user accounts, with estimated losses reaching \$100 million. However, it is well known that the highest risk for all organizations is accidental hacking caused by poor processes or a disgruntled employee deliberately damaging the systems (Wright & Altimas, 2015).

In 2010's cybersecurity due diligence consisted of asking a few questions in a short phone call (Farrell, 2014). A radical change has been made since. For example, Home Depot was hacked in 2014 through stealing email and payment card information of up to 56 million customers. Nowadays Home Depot's due diligence playbook includes penetration testing, and the due diligence is exhaustive (Nash & Minaya, 2018).

4.2 Role of Information security and ICT in M&A

4.2.1 Merging ICT Systems

Merging IT systems is discussed extensively in the literature. Merging information systems relates tightly to information security since each system bears risks.

According to TIVIA magazine (2023) The integration of IT systems poses a considerable challenge in M&A, primarily due to the complexity and diversity of the systems within each organization. The process requires early planning and a systematic approach to ensure compatibility and seamless operation post-merger. Common issues include the complexity of merging different IT infrastructures, data migration, and the integration of operational processes. These challenges are often underestimated, leading to complications that can jeopardize the merger's success.

Larsen (2005) states that the significance of ICT in an M&A process can be assessed based on the level of investment in ICT management and architecture and the extent to which the merged business operations are integrated thereafter. Larsen (2005) classifies the degree of post-merger integration into the following categories: selected consolidation, common enterprise systems, complete enterprise systems, and complete integration. Furthermore, the degree of post-merger business integration is categorized into the following types: holding company, network of businesses, shared services, and fully integrated.

Burke & Kovala (2017) noted that ICT is becoming crucial for quickly and effectively delivering the anticipated business benefits and shareholder value in mergers and acquisitions (M&A). IT integration is a complicated task with few established best practices. Key objectives in M&A transactions include ensuring a smooth day one, achieving synergy targets, and developing platforms that support future business growth. These objectives pose challenges related to data

migration, security, and support, thereby underscoring the importance of thorough due diligence and meticulous planning of ICT infrastructure.

Four categories of CIO level considerations by Burke and Kovala (2017):

- Strategy. Ensuring that business and IT are aligned, transforming strategic boardroom discussions into actionable and fair operational practices.
- People. Fostering leadership and communication skills while creating a comprehensive strategy for integrating corporate cultures.
- Control. Managing the large regulatory, information security, and governance standards necessary for merging companies.
- Delivery. Delivering the benefits of M&A through effective due diligence, realizing synergies, and successfully integrating post-merger (Burke & Kovala, 2017).

The Burke & Kovala (2017) research directly connects information security issues as one of the items of consideration is Control. The obvious regulatory standard is GDPR in the European context, and possible sectoral regulatory standards, for example, in financial sector regulation. Burke & Kovala (2017) raised a survey from 2014, that found 78% of respondents believe cyber security is not analyzed in great depth or specifically qualified as part of the M&A process. This number is most probably lower now in 2024 than ten years ago.

Burke & Kovala (2017) listed six focus areas that are common with successful M&A ICT integrations. The key to success lies in detailed planning. Successful preparedness puts emphasis on these focus areas:

1. Know your systems: An explicit knowledge of system architecture and what the most important systems are. This is key for pragmatic decisions when building integration roadmap.
2. Rationalize and prioritize: 75% of integration effort is to determine which systems to keep what data is important and how much integration is needed.

3. Communicate the synergy case: All parties need to have a clear understanding of synergies and drivers.
4. Decide on a dominant side: a clear driving force with single person ultimately accountable is key requirement.
5. Prepare a migration strategy: data migration to new platform requires delegate understanding of constraints, risk, compliance factors and skills.
6. Transitional Service Agreement: Business continuity is critical during the integration.

4.2.2 Post-merger ICT integration levels

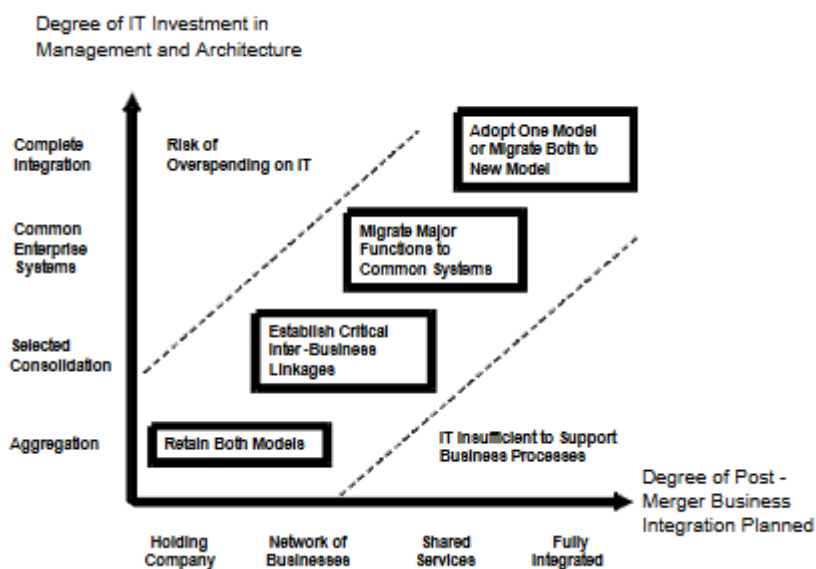


Figure 2 classification of post-merger integration levels

Larsen (2005) proposes a systematic structure of post-merger integration with different levels of integration, as in Figure 2 (Larsen, 2005). Not all combinations of the two dimensions are feasible because of overspending or insufficient business process support. The classification helps build an ICT vision of the post-merger ICT integration.

Benitez et al. (2018) state that A flexible ICT infrastructure enhances the capacity for ICT integration following a merger or acquisition. Standards that ensure compatibility and connectivity of ICT infrastructure support the integration of technical ICT infrastructure. Moreover, the capability to share, communicate, and connect various types of information, such as text, audio, video, and images, across diverse ICT components - both internal and external - to the organization, supports the integration of technical IT infrastructure.

The capability of ICT personnel to comprehend the business challenges of the merged firm, develop suitable ICT applications, and collaborate effectively in cross-functional teams with both ICT and business staff from the target company leads to the integration of ICT human infrastructure and ICT-business processes (Benitez et al., 2018).

4.2.3 Information Security inheriting risk blindly in M&A

Negotiations are highly confidential and sensitive, and CISOs are often notified of a deal only once it has been finalized. M&A can bring new information risk to a business, through new threat profiles, different customer and supplier bases, and internal upheaval in terms of culture, processes and systems used. Without an appraisal of information risk before finalizing the deal, the buying company blindly inherits that risk – with little understanding of any controls in place (Absalom, 2022a).

Absalom (2022) emphasizes the role of a CISO as an advisor to the decision-makers. The CISO needs to have conversations with the right people already in the planning stage to ensure the relevance and value of security. The challenge is to speak the language of the business to have effective conversations. CISO needs to be a critical friend to the business and offer valuable input at the right time in each stage of the M&A process. A Purely technology-focused approach often leads to ignorance and misunderstanding of CISO by the decision-makers. Therefore, CISO should see the big picture of information security as part of business and the relevance of information risk to the deal.

Absalom (2022) states that security leaders should recognize the relevance of information risk to the M&A deal. Information risk is only one of a broader range of business risks. Information risk is rarely an obstacle to completing a deal. Knowing the relevance and value of security, the CISO's

interventions are more effective in the scenarios where security considerations could be a deal breaker or have a significant impact on the value of the deal.

Examples of such scenarios include:

- Technology or security is the core value proposition of the target company (gaps in security would be a major concern).
- The deal would require compliance with new data privacy or security regulations (non-compliance by the target company may create significant financial exposure; or the regulations may prevent the acquirer from efficiently operating in the new market)
- The motivation for the deal is to acquire IP (if the target's IP has been compromised and leaked, it may significantly devalue the deal) (Absalom, 2022a).

4.3 Strategy and Information Security

4.3.1 Relation between ICT functions, management and strategy of an organization

Information and Communication Technology has traditionally been seen as just a technical function and all issues related to ICT as technological issues. As information security issues often appear as technical issues information security has often been tied to same department as ICT.

The strategic value of ICT has been discussed for the last 30 years. Henderson and Venkatraman (1999) introduced the Strategic Alignment Model that consists of four domains of strategic choice: business strategy, information technology strategy, organization infrastructure and processes, and information technology infrastructure and processes.

The role of information technology in organizations has evolved from its traditional 'backoffice support' function to becoming a vital component of organizational strategy (Henderson & Venkatraman, 1990).

Today, information security issues are seen as an organization-wide entity, which is affected by the organization's internal operating methods as well as, for example, information security

exercises carried out with companies focused on cyber security and their recommendations on the state of the organization's information security (Rignell, 2019).

Rignell (2019) states that Information security applies to all arrangements aimed at ensuring the availability, integrity and confidentiality of information. Within Information Security, Cyber security usually refers to the processing of information in digital form, and more broadly involves the entire network infrastructure as well as terminal devices, software and operating systems.

4.3.2 Relation between digital security and strategy of an organization

Digital security threats and incidents have surged in recent years, resulting in substantial economic and social consequences for public and private organizations, as well as individuals. Examples include operational disruptions, direct financial losses, lawsuits, reputational damage, loss of competitiveness, and diminished customer trust. An increasing number of stakeholders know the need to better manage the digital security risks to reap the benefits of the digital economy (*Digital Security Risk Management for Economic and Social Prosperity*, 2015).

An OECD report (2015) states that digital risks should be approached as economic rather than technical problems that call for technical solutions. Digital security can be addressed from at least four perspectives: technology, legal, national security, and economic prosperity.

Information security has traditionally been seen as a factor related to operational activities. Information technology and business expertise are not traditionally in the same place. In management groups, there is usually no information management, and the CFO represents information management (Porvari, 2012).

Hepfer & Powell (2020) studied three global companies that suffered from the 2017 NotPetya attack. They discovered that executives who have successfully navigated cyberattacks now regard cybersecurity as a top-level strategic priority. The executives acknowledged that their biggest mistake before the NotPetya attack was treating cybersecurity as merely an operational issue.

Organizational resilience to cyberattacks requires a fundamental shift in mindset: executives must consider cybersecurity a strategic priority, not just an operational concern, and see it as an opportunity rather than an expense. A mature cybersecurity strategy provides the foundation for safeguarding critical assets and business processes, promoting organizational learning, and identifying and capturing new strategic opportunities. It can reveal new strengths and fundamental weaknesses in leadership teams and organizational capabilities. (Hepfer & Powell, 2020).

Hepfer & Powell (2020) also examined common reasons for failing to recognize cybersecurity as a strategic priority. These reasons include delegating cybersecurity to IT, misunderstanding the strategic nature of cybersecurity risk, keeping attacks confidential, and executives prioritizing strategies based on their own areas of expertise. Executives who guided their companies through cyberattacks transformed their perceptions of cybersecurity from operational to strategic.

The four elements of organizational resilience to cyberattack by Hepfer & Powell (2020) is introduced in Figure 3.



Figure 3: Four Elements of Organizational Resilience to Cyberattack

The Nixu Cybersecurity Index Report 2023 raises business resilience as one of the main drivers of companies' cyber security investments. Security monitoring, security awareness, refining identity and access management (IAM) are top of companies' development objectives. Also supply chain security objectives are a high priority for both business resilience and regulatory reasons (NIS2 and DORA directives).

Best organizations prioritize risk management as a vital capability. A significant 76% include cybersecurity in their executive management discussions. The leading organizations allocate a more substantial partition of their total budget to cyber security (*NIXU CyberSecurity Index Report 2023, 2023*).

4.3.3 Information Security Policy, Information Security Management systems and Strategy

Paananen (2023) explains that Information Security Policy (ISP) holds different meanings in computer science security and management information systems security. Many research articles lack a clear definition of ISPs, and no single definition has become predominant. In computer science, ISPs refer to technical policies and information systems management. The varying perceptions of risks, resources, and management styles among companies lead to diverse definitions and functions of ISPs.

Paananen (2023) states that, in a narrow sense, an IS policy document represents a declaration by key management figures (such as the CEO, Executive Board, or Minister) outlining their beliefs, goals, rationale, and general approaches to achieving desired outcomes in the field of information security. The intention is not limited to achieving security objectives (integrity, availability, confidentiality, CIA) but also ensuring that the organization reaches its goals despite accidents and attacks (Paananen, 2023).

Paananen (2023) states that the information security policy can be derived from strategic risk management requirements, allowing strategic-level decision-makers to use the policy as a tool to mitigate risks to the company's information assets. Besides risk prevention, security policies can also function as a recovery plan for materialized risks.

Sadok et al (2020) states that corporate information security policies are often disconnected from actual day-to-day work processes or are not on very high priority – especially in SME sector.

The workforce finds ways to bypass security controls to do their work effectively. Workarounds indicate that information security and other work objectives are not aligned, often stemming from a lack of information security awareness or understanding of actual working practices. This misalignment leads to new vulnerabilities, suggesting that everyday security issues should be viewed as emergent consequences of human activities. Therefore, separating social and technical aspects is neither desirable nor advisable. The need to align security and business processes is a long-standing issue in security management. Many examples demonstrate that effective security measures must be established within a clear organizational context (Sadok et al., 2020).

Sadok et al. (2020) argue that ineffective security often arises because security practices are developed without considering the needs of the workforce and business processes. Proper communication of security controls to employees is essential. Additionally, the CISO plays a crucial role in aligning security measures with business requirements.

4.3.4 Information security skills in company board and the role of CISO

Company boards are the initiators of M&A processes, so there is a reason to touch on the company board's skills. Sims (2023) had found in his research that cyber security issues get more significant amount of meeting time compared to previous years. Many boards have noticed the skill gap in security, but they have not defined what experience the role requires.

Sims (2023) article discusses the role of board member as cyber strategist. That person should be able to align cyber security goals with broader business objectives. This requires strategic level thinking of reducing risks in achieving company strategic objectives. Other listed skills are good communication skills making the vast variety of consequences of cyber risks, and their potential influence on the company, understandable to the board.

A good quotation from Sims research: As one CISO and board member put it to us, no one on the board truly understands what it means to have 200-plus unpatched vulnerabilities, but they do

understand what it means to have an aggregate liability of \$400 million if those vulnerabilities are not addressed (Sims, 2023) .

4.4 Designing product and service offerings for cybersecurity from the start

Pearlson & Huang (2021) presented good viewpoints in their research for combining cybersecurity tightly to the design process and company product and service offerings.

Designers and managers typically underestimate how severe the consequences of cybersecurity vulnerabilities can be. Increasingly, cybersecurity is becoming a de facto requirement and thus a key selling point (Pearlson & Huang, 2021).

Pearlson & Huang (2021) found that there are three typical ways to tackle cybersecurity:

1. Bolting on security fixes. This means performing vulnerability testing, penetration testing, and quality control testing. When a vulnerability is uncovered it is sent back to the design team to be fixed. That might mean undergoing costly re-designs or finding different but more secure components.
2. Incorporating secure development lifecycle processes. When there are parallel processes, there are specific steps the designers can take to ensure that the design and prototypes have the right security built in. There is still the risk of having to scrap an early-stage design and start over.
3. Embedding security consultants. Having security experts work with the design team raises some challenges. The security experts are not necessarily always available and even more challenging is that security experts do not necessarily understand the product at the level necessary to offer helpful design advice. At the same time designers themselves need to have enough knowledge of security needs to build in cybersecurity from the start.

Cybersecurity becomes one of the basic design criteria, similar to manufacturability, usability, quality, cost, and the many other elements that are part of any design process. Designers with security backgrounds reported that they made decisions on tools, libraries, and components to use in their product designs based in part on how secure they were (Pearlson & Huang, 2021).

Pearlson and Huang (2021) found four mechanisms that support incorporating cybersecurity into the companies' offerings.

1. Performance appraisals should be tied to cybersecurity. To drive a change in the attitudes of employees, security metrics must be visible to leaders. Leaders must be ready to delay or reject the release of digital offerings with insufficient cybersecurity built in and hold the development team accountable.
2. Give visible recognition to employees who engage in positive cybersecurity behaviors. Still, recognition can be a simple thing and still effective.
3. Train employees on security in addition to using experts. Employees need basic training on how to design cybersecurity and should be reminded that it is their responsibility. Agile development processes must also include stories based on cybersecurity requirements. Safety nets, testing activities, and experts in secure development life-cycle processes are still needed to supplement the initial security designs, but designers must have enough knowledge to do the first pass.
4. Deliver strong and frequent messages to increase awareness of cybersecurity needs. The key action here is to continually remind everyone involved in the product development process how important cybersecurity is so that they internalize that belief and align their personal attitudes with the need to develop secure offerings. Building in cybersecurity earlier in the design process makes the whole product development process more effective.

4.5 M&A Risks

Although growth strategies built on mergers and acquisitions are popular, they have substantial execution challenges, 40% to 80% of mergers fail to meet objectives (Dunbar, 2014).

Dunbar's (2014) five-year study of 94 mergers from 2004 to 2008 uncovered three major findings. First, leadership capabilities in acquiring companies predict M&A success, specifically in thought leadership, results leadership, and people leadership. At the same time leadership in target companies is equally important. Second, the study identified seven specific leadership competencies in acquiring companies and four in target companies as indicators of M&A success. Third, the effectiveness of senior leadership in acquiring companies and middle management leadership in target companies has the most significant impact on the overall success of mergers.

4.5.1 Points of Failure in M&A

The very common question in numerous research papers and journal articles is ‘why do M&A deals fail?’. Burke & Kovala (2017) states that things can go very wrong during an M&A transaction. The impact of failure is long-lasting: financial losses and company reputation and regulatory issues (often in the form of lawsuits). All these will bring negative publicity and are difficult to deal with simultaneous financial losses. From the ICT viewpoint this could mean system outages for critical systems, compromised system integrity or data loss or theft.

Sherman (2018) states, that most deal killers can be put into one of the following major categories:

- Price and valuation
- Terms and conditions
- Allocation of risk
- Third-party challenges
- Cold feet due to oscillating financial conditions.

5 Results from the interviews

5.1 Overview

The integration of IT systems, along with legal, operational, and cultural considerations, plays a critical role in the success of mergers and acquisitions. Proper planning, thorough due diligence, and a systematic approach to integration are essential for tackling the challenges associated with M&A. Understanding the systemic complexities and addressing them proactively can significantly increase the chances of success in these ventures.

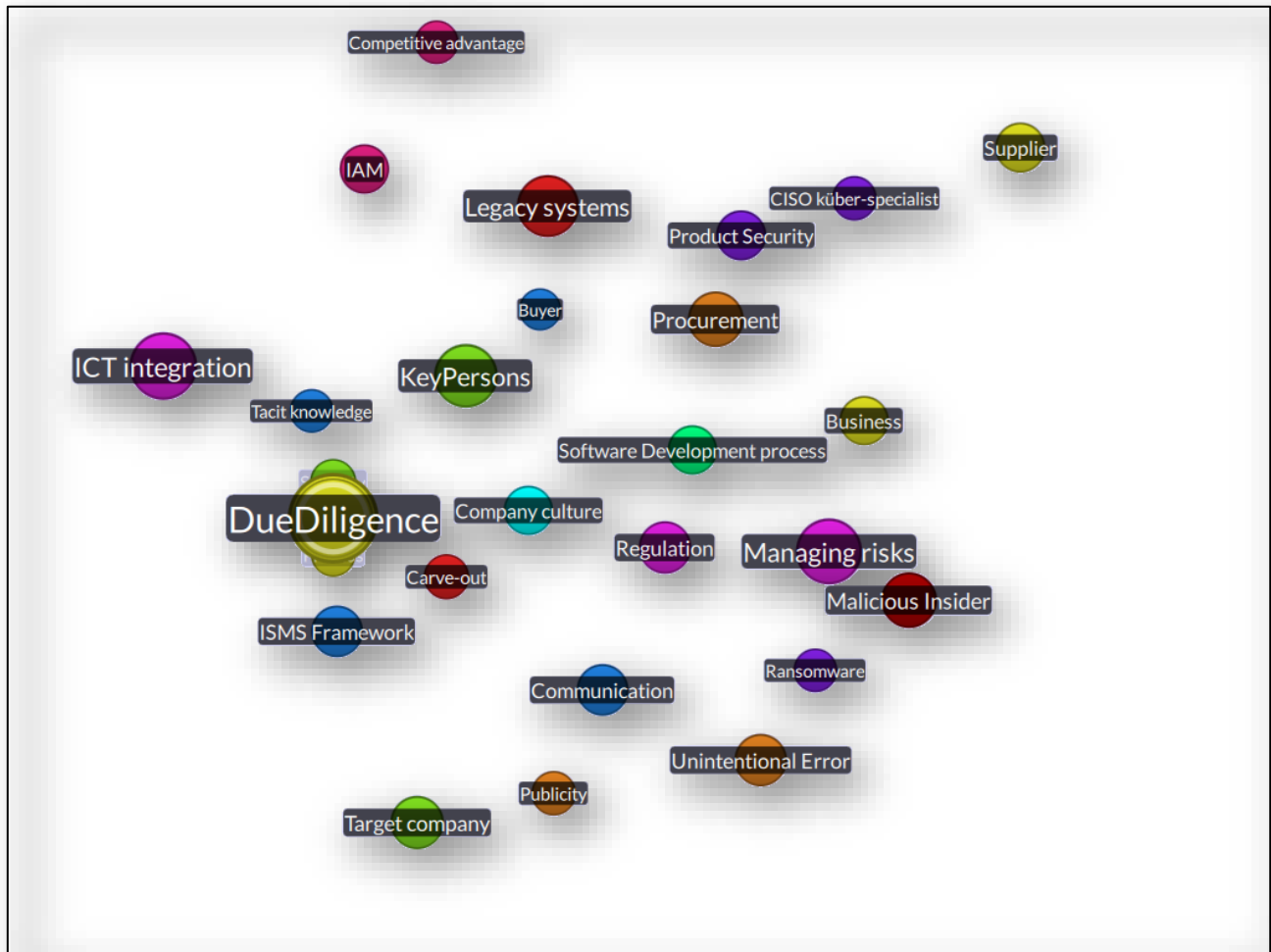


Figure 4: View from the Quirco screen capture demonstrating the subjects that raised in the interviews.

As Figure 4 well demonstrates, the discussion areas varied from due diligence process to ICT infrastructure, ICT skills and information security skills.

The facts of interviewed persons and their background

Number of interviewed persons	10
position	Director:1 CISO: 6 CIO: 2 PO: 1
Number of years of expertise in information security	10-20 years.
Industry sectors of the companies	Industrial services: 2 Technology: 4 Financials: 3 Consulting: 1
Company type	public company: 5 private company: 5

5.2 Due Diligence process.

The due diligence process typically has different tracks: legal track, business track, financial track, and ICT track. Typically, there is quite a tight timeframe when all the due diligence activities should be performed. Information security requirements depend a lot on the target company's size and industry. An information security assessment could be done according to an information security framework. It is also possible to do open-source intelligence and search the web and the dark web to figure out a company's attack surface.

The common recommendation raised from the interviews is to keep a helicopter view of the information security due diligence process. The target company's systems are not perfect, and neither are the buyer's own systems. Technical details and architecture are important, but one should not get stuck in the details alone. The more important thing is to see the target company's overall information security risks.

5.2.1 Technical Information Security Needs Improvement

One of the interviewees gave a very strong message regarding technical auditing in Nordic countries: "In my opinion, the technical side of data security is hopelessly behind compared to larger countries. For example, in the UK, it is already starting to be part of the due diligence process. Especially when due diligence shows risks, M&A processes already look at the whole from a technical or deep technical point of view. In the Nordic context, the technical side still only scratches the surface. In other words, full verification of, for example, whether the control is in order or how widely an SIEM has been deployed or something else where the answers are usually "yes" or "no" instead of "how". In my work, I have seen that the technical side has come to the fore at the point when the buyer is really worried about whether everything is in order. Time-out and scope extension are often taken separately to perform this kind of technical verification. "The interviewee continued later this by stating that there are good exceptions in companies who have inorganic growth as their strategy.

5.2.2 Due Diligence to serve pre-integration planning

Some interviewees raised significant points about the due diligence process: Due diligence should feed information to the pre-planning phase so that information security is not jeopardized. This also concerns ICT integration and procurement since due diligence could bring important aspects to choosing technical solutions and overlapping agreements. The information security analysis should have a wider perspective than just a security audit or outsourcing agreement price tag. The analysis should go beyond Excel sheets towards a more holistic view of server pre-integration.

5.3 The topics of discussion when assessing target company's security

There was no clear list of things provided from the interviewed subject matter experts. One must keep in mind that the interviewees represent very different companies, some of them actively grow by M&A: s and others perform M&A: s very seldom. However, certain topics were commonly named:

- Security policy and management
- ICT policy
- Incident management and public security footprint

5.3.1 Preliminary questionnaire and meeting

Before the meeting with the buyer and target organization, there is typically a questionnaire regarding information security that is sent to the target organization. The target organization answers with their best knowledge.

This subject was discussed widely in the interviews. The three interviewed experts from companies that perform several M&As each year explained that when the target company is an SME company, they typically don't have a comprehensive information security management system. Rather they just have some guiding policies for information security they follow.

One interviewee discussed this topic from the target company's perspective. The person's experience was that Nordic buyers ask clear and specific questions but accept high-level answers. On the other hand, North American companies ask very generic questions but expect quite detailed and structured answers.

All respondents emphasized that the preliminary meeting should not be like a police interrogation. Both parties should have a constructive approach and willingness to build trust between the parties. One interviewee underlined that these meetings are possibilities to sell the positive side and the synergies of the coming merger to both parties.

5.3.2 Security policy and management

Some security policies were named: ISO/IEC 27001, NIST, and ISF. The three interviewees, whose companies perform several M&As annually, discussed the security policies in more detail. They emphasized two things:

First, SME companies seldom have a formal security policy. The security policy can be systematic though.

Second, when the target company is merged and the integration starts, the information security management systems must be applied immediately after the handover. The buyer takes all the residual risks simultaneously.

When asked if joining two different ISMSs is challenging, all interviewees answered that there are quite a lot of similarities, and there are conversion tools available, too.

5.3.3 ICT policy

Most of the interviewed subject matter experts emphasized that Information Security and Information and Communication Technology are two different things, although there are some relations through information being stored in digital form.

The most important thing is to get a realistic picture of the target company's ICT policies. Many interviewees said that budget is a good benchmark for validity. The total amount spent and what the money is spent on says a lot.

The division of work and decision-making is another good indicator of the quality of the ICT policy. Worst-case scenarios are called “paper tigers,” where everything seems okay on paper, but in real life, an understaffed ICT function takes care of information security on the side.

5.3.4 Incident management and public security footprint

Companies that acquire target companies frequently tend to use open-source intelligence to build a footprint for the target company. This does not mean penetration tests but rather public scans

within the legal framework, which are added with some information searches from the dark web. It Would be a clear showstopper for the whole M&A if, for example, the customer database had leaked outside the company.

One of the interviewees explained how they have developed ways of politely finding out if the target company has suffered any security incidents. When asked directly if there have been any security incidents, the answer is 100% “No.” Typically, the target companies don’t know their vulnerabilities well, but an outsider’s view of the security footprint can be eye-opening.

5.3.5 Nature of Assessment Meetings

The interviewees emphasized that no companies have perfect information security. There is always room for improvement in any company. The assessment meetings during the due diligence process serve the buyer in confirming that the target company is worth the money. A common prejudice is that assessment meetings resemble police interrogations. The reason is obvious psychologically because the participants understand that due to the M&A their current job could end.

The interviewees representing companies frequently performing M&A explained that it is important to build cooperation, team spirit, and trust in these meetings right from the beginning. The result could ideally mean that the target company could carry out previously too expensive security controls because the M&A budget makes it possible.

5.4 Product security vs organization security

The interviews revealed that information security should be divided into two categories: organizational information security and product security. The latter refers to security analysis of the target company’s products or services with digital components. The interviewees, who represent the software industry, explained the details of how they perform technical security tests, software library analysis, and other activities directly related to the product. However, the software development process itself is partly organization security and partly product security. That could explain why product security was not named separately.

The term product security was brought up as a term with interviewees, who talked about tangible products that have a significant integrated digital component. However, product security is relevant for fully digital products like software and online services too. Many companies understand what information security means and could even have certifications like ISO 27001 or equivalent. This certifies that the organization has a certain level of security in the structures. But this still leaves one question open: “How to ensure, that the code pushed to production is secure?”. This question belongs to application security

The interviews brought up software security in various ways: One company does very lightweight organizational integrations with the target company, leaving it to continue its current business with very mild modifications. The first and most significant change is the implementation of software security standards. Another company does more comprehensive integration with the Information security management system, new infrastructure, and software security standards.

5.5 Tight timeframe and urgency of the process

Many of the interviewees mentioned the tight time frame. There is, however, a rationale understanding that tight schedules mean heavy prioritizing, and not everything can be tested. A direct quotation from one of the interviews: “You just can’t find all security issues within the timeframe”. Due diligence tracks that concentrate on information security must emphasize finding the most significant areas of information security within the given timeframe.

A question remains open: how much does the buyer blindly accept risk?

The tight schedule means a great amount of extra work for the target company’s information security function. The audit and communication with the buyer side information security function/track requires extra reporting and meetings along with the line work of that function. The amount of work depends on the information security maturity level of the target company.

5.6 Business culture

The discussion subjects were formed to find answers to research questions. However, most of the interviewees raised the company culture as a significant factor on many occasions. The company culture should promote co-operation and build trust and rapport with the different stakeholders. Also differences in business culture between the USA and the EU were raised in over half of the interviews. There is a keen relationship with these two market areas, so cultural differences are obvious.

5.7 Treating inherited system risk

There is always inherited system risk when two companies merge. The inherited risk is in the form of legacy systems, procurement risk, personnel risk, and supply-chain risk.

5.7.1 Legacy systems and technology debt

The interviewees gave quite expectable answers to treating the risk involved in legacy systems. Most of them emphasized that the term legacy system is quite vague and leaves a lot of space for interpretation and speculation. The interviewees narrowed the legacy systems to systems that are old or end-of-life status.

In the beginning, the buyer should know the possible attack surface of the legacy systems and also consider the availability matters of such systems.

There is a continuity risk if the system is old and hardware components are hard to find or slow to replace. The software is also a challenge, since there might not be updates available or even a skilled workforce to repair old software. Therefore, the risk mapping of legacy systems is vital. The mapping should also include the human skills factor – whether it is in house or outsourced. Legacy systems are more sensitive to risks cumulating from key persons availability or existence. There is lot of tacit knowledge involved in maintaining mature or end-of-life systems. This tacit knowledge should be documented or otherwise transferred, to make sure the knowledge and skills are not in the hands of one person only.

Other types of legacy or technology debt mentioned was software stack life cycle. When for example the core version of the used programming language or other component in the software stack is outdated or old the costs for modernizing could turn out to be quite high or the redesign process take too long. In these cases – especially in software industries – the technical and cash flow analysis could prove that the too high operating expenditures is a reason to stop M&A process.

Few interviewees raised poor IT governance as a risk when discussing legacy systems. Poorly managed CMDB and floppy processes are issues that come up when legacy systems are discussed. They stated that quite often, legacy software goes hand in hand with poor IT governance. This could also be expressed with the term technology debt.

To be fair, the buyer is not necessarily more modern than the target company. Many interviewees commented that both parties should be analyzed equally and the best tools and practices for integration should be chosen regardless of origin.

One of the interviewees had experience of a situation where the information security gap was significant, and that also reflected the due diligence process. The information security due diligence was done on paper only, without a meeting with the partners, which was quite confusing in the target company.

5.7.2 Procurement risk

The target company typically has contracts, the contents of which should be carefully clarified. The legal track in the due diligence phase typically processes the contracts at a detailed level. If these contracts are not subject to due diligence and there are dependencies on the target company's essential processes, there is an increased continuity risk afterwards.

Software and cloud service licenses typically fall into procurement risk categories. The interviewees recommended comparing similar contracts that both buyer and target have in common. Some cases revealed significant pricing differences. In such cases, it is worth considering whether to keep or terminate contracts.

Information security risk in procurement is a challenge. One expert interviewed raised a question, “How is information security addressed in the procurement text?”

5.7.3 Asset management

Some interviews revealed the various levels of asset management in companies. It is not surprising that some companies have an ICT component or outsourced services that have fallen outside asset management databases. This could, for example, be an open-source security component that someone just installed but forgot to add to the CMDB configuration.

5.7.4 Residual Risk Treatment

The process of treating residual risk is theoretically a two-way process: accept or mitigate risk. Typically, the mitigation follows the PDCA model.

Many of the interviewed information security specialists raised residual risk acceptance as a special case. Accepting risk is a management decision, and it can be either good or bad. Risk acceptance is an easy way of dealing with residual risk. The interviewees raised a sentence that is too commonly heard: “So far, nothing has happened, and let’s hope nothing happens in the future”. However, the management gets a clear calculation of the opportunity costs of solving such incidents in case the risks are realized to incidents. The price tag for the incident can turn out to be quite high although the probability could be quite low at the same time. There are also many secondary effects, like company continuity, amount of extra work, company reputation, loss of customers and possible law suites and legal penalties, that must be added to the incident calculation.

Management decisions are often based on a subject matter expert’s presentation to the board. The nature of digital risk is often difficult for a businessperson to grasp since full understanding requires specialist skills. Therefore, it is vitally important that the risk and its consequences are clearly communicated to the board to enable them to decide based on facts. A quite common comment from almost all interviewees was that a CISO needs good communication skills.

One expert interviewed crystallized risk acceptance: “Accepting risk is a cheap, quick fix that leaves technical debt.”

5.7.5 Unintentional error

Unintentional errors can occur because humans make mistakes. The reason for error can be a short time frame with limited rights to communicate with other stakeholders. This could be a very small misconfiguration in endpoint, server or cloud, or network. The overall complexity and large of today’s ICT environments leave room for errors. The best mitigation is to have clear instructions, playbooks and processes. With rather simple process improvements that apply cross-checking and four-eye-principles (meaning two persons control each other’s work process) can significantly decrease the probability of errors.

The nature of M&A operations is quite unique. Each time two unique organizations merge in some way, but there are never two projects that would be 100% similar. Also, the stakeholders in each project differ. Therefore, there is a risk that some processes or controls can fall between two chairs, meaning that both parties think that the other party takes care of that process. Again, the best mitigation is proper planning.

One interviewee suggested reviewing the time frame of the M&A process to mitigate unintentional errors in three ways: First, include the information security function early enough. Second, the project manager should oversee that there are enough alignment meetings with discussions—not only status reporting. Third, there should be enough idle time between tasks to reflect on what has been achieved and whether everything that needs to be included has been included.

5.8 Paper Tigers

An interesting term “paper tiger” was raised in four out of ten interviews. This refers to a company with good information security documentation but appears to be the opposite when security scans or interviews with the company are performed. Further, these companies tend to have immature information security policies, lack of cybersecurity controls or just sloppy ICT governance.

5.9 M&A Activity Activates Criminal Actors

Eight interviewees commented that companies that are either buyers or targets in the M&A process also have an increased risk of being a target to criminals. First, when the companies inform about the M&A through web pages and press releases, there is an increased risk of targeted phishing campaigns just because the criminals try to seize the hectic time in both organizations. When the process continues, and possible ICT integrations are performed, there is a risk of malicious outsiders trying to illegally enter the systems using various techniques.

5.10 CISO and information security organization involvement

Information Security forum addressed the information security risks in mergers and Acquisitions by publishing a whitepaper (Absalom, 2022). The figure's key message is that the CISOs hear from the M&A process at a very late stage. Information security can have a significant impact on the deal.

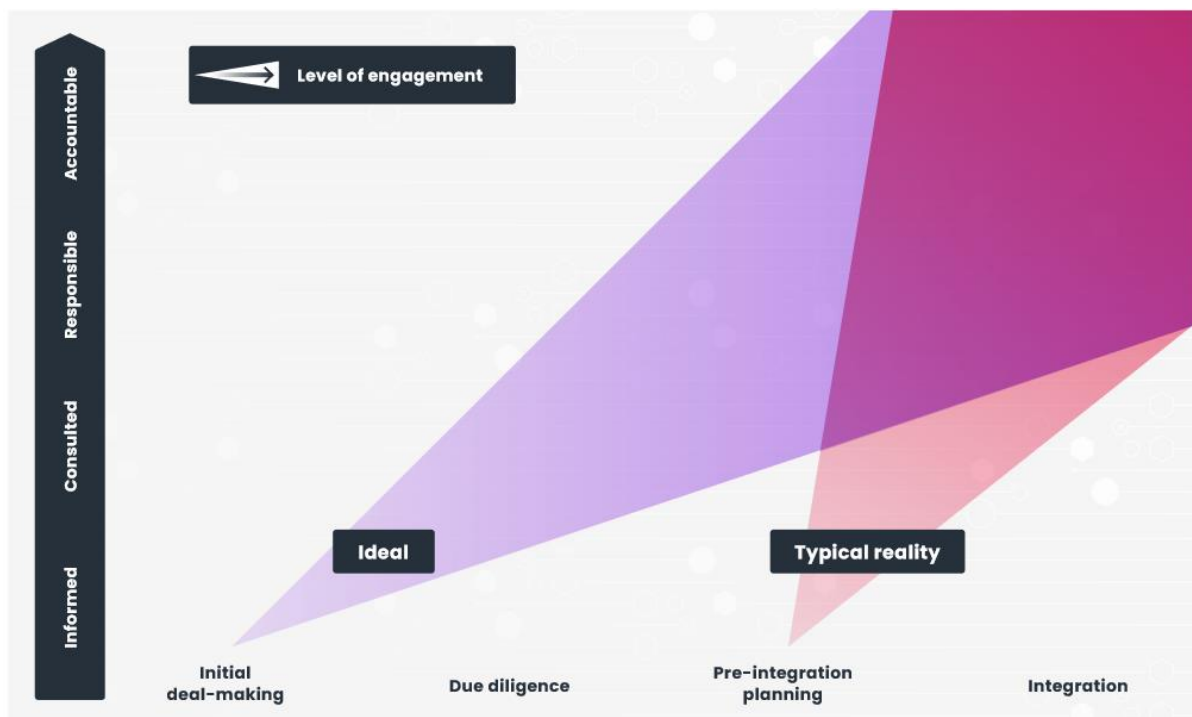


Figure 5: The four stages of M&A activity - and the extend to which CISOs are involved

The same matrix was used when interviewing the subject matter experts in information security. However, the ISF results were removed, and the interviewees were asked to mark what they considered to be a realistic process and ideal process.

The ISF results were quite similar in Finnish context. However, the realistic status seems to be better since CISOs are typically involved on some level (consulted or minimally informed) already in due diligence stage. None of the interviewed experts considered pre-integration planning to be the starting point for CISO involvement.

Another clear observation was that this matrix and its use are very different if viewed from the seller's or buyer's viewpoint. A suggestion was to draw two separate matrixes – one for each viewpoint. The common view was that this matrix was implicitly from the buyer's perspective.

The RACI matrix principles are explained in Appendix 2.

Accountable				G
Responsible		D	E	F
Consulted	B	C		
Informed	A			
	Initial Deal Making	Due Diligence	Pre-Integration planning	Integration

Figure 6: The four stages of M&A activity and CISO role - results of the interviews

In figure 6 the letters A to G indicate stages where interviewees shared a common view. Not all cells have a letter, which means that none of the interviewees selected those cells.

A clarifying summary before diving into the details of each letter and the stories to justify the choices: All interviewees agreed that early involvement would be recommended because it positively impacts the analysis. Early involvement of security experts also prevents the process from stopping earlier rather than at the last moment after all the efforts made for due diligence, in case there appears to be a showstopper based on security issues.

Also, companies that routinely acquire other companies as their growth strategy tend to have preprepared processes and playbooks to ensure positive M&A results.

5.10.1 Stage A: Informed In Initial Deal Making

Typically, CISO is not involved in this phase. Most interviewees recommended that CISOs should at least be informed on a general level to be prepared for future work, and some recommended stage B (Consulted) directly. For companies with M&A as their growth strategy, the CISO is typically informed.

5.10.2 Stage B: Consulted In Initial Deal Making

This stage had reasoning among the interviewees that a CISO would have enough time to organize the extra work. CISO could also advise the participants to ask and look for information security related materials significant for the deal.

5.10.3 Stage C: Consulted in Due Diligence

The CISO can bring an understanding of which things should be paid attention to regarding information security. The interviewees believed that both realistic and ideal situations are consulted. The reasoning for this is that information security is an activity that supports business, in which case business is responsible, and information security plays a consulting role for business.

5.10.4 Stage D : Responsible in Due Diligence

The CISO acts as a point of contact, who knows how to emphasize and prioritize the most important issues in information security. Information security expertise is required to understand and seize the risks. There were clear differences in nuances, but the big picture was same: the role

of information security is seen as supporting business, and thus ownership is seen as belonging to business.

5.10.5 Stage E: Responsible in Pre-integration planning

There are still a lot of dependencies in pre-integration, which must be considered to stay within the given time window. For example, let's outline what happens during the first hundred days, so that information security doesn't stray into side paths. Business must be put first, but with data security in mind.

There is a difference in the answers, as some of the answers were a bit imprecise. It was concluded that the information security organization is responsible for the information security framework and controls, but the risks are owned by the business.

5.10.6 Stage F and G: Responsible or Accountable in integration

As explained in stage D and E, the role of information security was a point of discussion here. Information security function is a business enabler or support function to business. At this stage, responsibility was expressed as responsibility for maintaining the security framework that other actors or functions could follow when performing integration. The word responsible was mentioned, but the meaning behind the word was that information security is consulted, if the other functions needed interpretation of controls, or informed that required controls are in place.

5.11 The relevance of information risk to the deal

Information security risks are not necessarily deal-breakers if they can be fixed. The financial impact of repairing or improving information security is then more decisive. If the case, that an evil actor is already in the target company network, causing security and privacy breaches, for example, company customer lists or IPR material on sale in the dark web, the company could be worthless.

Known risks are maybe affecting the price tag of M&A deal but as they are known they can be measured, mitigated or accepted. The unknown risks are worse. As one of the interviewees stated: “A vulnerability doesn’t wave a hand as signal or risk. A vulnerability just exists, and one day a bad guy finds the vulnerability and uses it for bad things”

An investor can compare candidate target companies and draw conclusions that well-managed information security increases the value of the company.

5.12 Identity and Access Management

Identity and access management (IAM) is a challenge in every M&A these days. When two companies merge, there are two—possibly quite—different ways of performing IAM. This leaves questions for the companies subject to the process to answer: Which technology base is used for IAM, who will take care of the IAM process, and how fast the IAM should be up and running?

Some comments from the interviews: “For example, Microsoft and Google are now compatible.”, “In cloud services, Amazon and Azure already operate with slightly different logic. A key question is how to combine the two”, “There are dependencies between IAM and other systems and those access rights limitation mechanisms always create challenges.”

One quotation emphasizes the significant role of IAM: “In large enterprise M&A processes, IAM should be a high priority because a quick fix can cause huge expenses in the future. Therefore, proper IAM planning is justified.”

5.13 Industry-Specific or General Regulations

When discussing regulations, the typical discussion referred to legal questions, and the legal track in the due diligence track was mentioned. Also, a very common topic of discussion was GDPR and privacy issues that might come up during the process.

Some interviews touched on the heavily regulated financial industry and publicly listed companies that must follow stock exchange rules and regulations related to listed companies.

Rules and regulations include sanctions and other disciplinary procedures for organizations that don't adhere to them.

5.14 ICT Integration

Carefully done due diligence improves integration planning and building risk registers, too. The residual risk is known already before the integration process starts.

There are numerous ways to implement ICT integration. Typical ways of implementation that the interviews raised are:

- Integrating the target and buyer by building integration layers
- Leaving the target company to its own isolated entity, but adding policies, and security controls
- Importing target company's data to buyer's existing ICT systems.

ICT integration is not an overnight process. The interviewees listed risks that fit the CIA-triad (Confidentiality, Integrity, Availability) and emphasized that the process takes time. First, Confidentiality risks increase if, for example, IAM is not correctly configured. Second, Integrity risk increases when data is merged due to, for example, poorly tested import scripts of equivalent. Availability risks emerge when business process flow has to stop due to system downtime when correcting the confidentiality or integrity-based issues. A recommendation from the interviews was to plan the integration properly and realistic scheduling.

Almost half of the interviewees raised the possibility of improving ICT infrastructure in this phase. The strategic decision for integration is made, which means it would be easier to budget for significant changes. If the technologies from both buyer and target are evaluated realistically and unbiasedly, it would even be possible to pick the best tools and practices from both sides.

5.15 Key-persons leaving the Company

This subject was very widely discussed in the interviews, although the initial question was, “Is this side effect an issue?” The responses discussed human reaction, tacit knowledge, and employee engagement.

Personnel turnover is usually quite high with business acquisitions. A human reaction to significant changes in work life is assessing the current work role. Change negotiations often ignite employees, who are not necessarily subject to those negotiations, to evaluate their careers and make a career move.

A poorly managed acquisition leads to more employees easily leaving. A very direct comment: “It's bad planning if you don't accept the fact that in that situation people leave.”

Company culture as the reason for leaving was also raised in one interview: “When a startup company is bought, and the culture is an even bigger upheaval when they have to move to a corporate culture.”

When key persons leave a company while the M&A process is ongoing, there is a lot of tacit knowledge leaving the company. The interviews highlighted the importance of documentation of tacit knowledge – or all information regarding the work processes and systems in general. According to one CISO, it is rare, that a company makes most of the leaving employees by asking them to document their knowledge and work. What employers often do, when the notice of termination comes, they start looking for a new one, but we don't have that dialogue with the resigned employee to perform the documentation of tacit knowledge.

One interviewee expressed very clearly: “You just know that you're missing tacit knowledge, but you figure it out too late - that's it.”

The most extreme example was when three retired people were recruited in another Nordic country to maintain one rare legacy system so that the transition and legal responsibilities were fulfilled.

Another quotation that brings up the brutal reality in trying to get keypersons back: “Since it was a very critical process, we had to recruit a few people back from a competitor. They were not willing to return with the wage they started with, but I think they tripled the request.”

A good rule from experienced CISO: “Don't buy an organization where the documentation is so bad that it can't handle the departure of a few key people.”

5.16 Infosec Communication Skills

Surprisingly many interviewees mentioned communication skills. Initially, communication skills were not included in the thematic questions. However, many interviewees raised communication skills as rare but much needed set of skills. This quotation tells a lot: “In my opinion, ICT is, or IT in general, has already gotten out of its own silo a little to the rest of the management and to talk about the same things. What you see in the M&A work itself, even between the teams, is that information security professionals are still a bit of a troll. Could you say that they understand and can bring - or when they know their own pockets very well - and their own nuance very well. But when those things should be communicated to others in such a way that they understand what this means, everything you have just said in the last fifteen minutes, then there will be a problem, and this is the big deal.”

Another interviewee mentioned that not everyone can participate in M&A operations. In due diligence, a technical person can get far and find deviations. To make due diligence effective, a person should also be able to communicate with people at least on some level. A great deal of situational awareness and the ability to build rapport—and maybe even build positive attitudes towards the buyer in target company employees' minds—are rare but needed skills.

6 Discussion and conclusions

How are CISOs involved in M&A process? The literature review reveals that CISOs often participated in a very late phase of the M&A process. What if the CISO were involved earlier?

The question of CISO's or information security function's involvement in M&A was analysed from several different angles in the interview. When asked if the involvement is typically too early or too late, the spontaneous answer was that the CISO / information function should be involved earlier. However, a deeper discussion with the interviewees opened more perspectives on the matter. When the interviewees placed in RACI matrix with phases of M&A – based on the ISF article - it seems that the CISO or information security people are being involved at an earlier stage than the ISF study showed. However, the sample in this study is relatively small compared to the study conducted by ISF, so it is perhaps indicative. ISF's research was done a few years ago, so it is also possible that a strong development has taken place over time. A further study with large enough target group would give more reliable answers to this.

At the very beginning of the M&A process or in the pre-preparation phase, the CISO or information security function does not need to be aware of possible M&A plans, unless there is a rational reason for informing in advance. The interviewed information security experts underlined that information security is not the core of the company's business, but rather is positioned as a

Information security has a increasingly significant part in the due diligence process. It is dealt with in its own track in the due diligence process with contact points with legal track and ICT track. It is also possible that the buyer can do OSIT and security scans towards the internet facing parts of the target company to be able to see potential vulnerabilities. Information security issues can have a significant impact on the value of the company being bought.

In addition to the target company's information security, product data security also proved to be important in the interviews between the target and the buyer. More and more products or services have a digital component, which greatly impacts both the target company and its products.

The appropriate level of security and due diligence is a complicated question. Basically, the due diligence process does not offer enough time to handle everything possible related to information security. There is always minimal time in the process. It is important to get honest answers about the state of information security from the target company. Mere yes or no questions are not enough. There needs to be practical ways to validate the documentation.

Prioritization is important. Returning to the basic principles of information security, i.e., thinking about the most critical thing to protect and how it is protected. On a case-by-case basis, the technological solutions of the target company and the maturity of information security affect what is prioritized in the due diligence process.

6.1 Limitations of evidence

During the research process, the RACI matrix was used to determine whether the CISO or information security function is involved early enough in the M&A process. The positive side of the RACI matrix is that the interviewees were familiar with it. However, when the discussions during the interviews dealt with the buyer's or target's side, the two-dimensional matrix turned out to be missing one dimension. The matrix would look different from the target company's side than the buyer's. The matrix was, however, comparable to the ISF survey when it was used in its current form.

6.2 Discussion

Summary of Findings and Comparison of the Results with Literature

The research question of how CISOs are involved in the M&A process was approved to be relevant. The findings from this study indicate that the CISO's role has improved compared to the literature review, indicating a late, or rather too late, phase of the M&A process. This earlier involvement aligns with the recommendations of several scholars (Absalom (2022), Burke and Kovala (2017)) who advocate for the early integration of information security functions to mitigate information security risks effectively. However, the literature also points out that there are still gaps in the systematic application of information security during M&A processes.

This study reveals the interviews also covered the second research question of how information security is considered in the integration process. There seem to be information security activities in the due diligence process that

The literature review didn't clearly mention product or application security. The M&A process is seen as the merging of organizations, and less attention is given to the products and services and their digital security components. The expert interviews revealed the significance of high product security in the target company and the fact that poor product security could be a deal-breaker.

The reviewed literature did not pay much attention to information security due diligence. The expert interviews revealed certain similarities between it and information security auditing in supplier management, but obviously, with different emphases.

Outside, but tightly related to, information security is the fact that the M&A process causes key people to leave, and a lot of tacit knowledge walks out of the doors at the same time.

Organizations that are more experienced M&A players understand how to keep this fact in the risk register and mitigate the risk with various ways of compensation.

The literature mentioned unintentional errors but provided no practical details. The interviews revealed that unintentional errors could increase information security risks and costs. Suggested

ways of mitigation were good project management, systematic communication within the project, and proper idle times to avoid multitasking and stress.

The interviews covered the second research question, which concerns how information security is considered in the ICT integration process, quite well. After the due diligence phase, both parties should have a good understanding of residual risk. When the deal is closed, the target company hands over all the risks to the buyer. This is a critical moment since all the financial and legal responsibilities the risk causes are also handed over. As one of the interviewees put it very well: "The risk just lies there. It doesn't give any signals until the risk is realized when a crook utilizes a vulnerability, or something else happens."

Obviously, the level of integration means different kinds of risk treatment, as the interviewees emphasized. The minimum is when just the data from the target company is imported into the buyer's systems, and all software and hardware is replaced with the buyer's equipment. If the data transfer process is managed well and data confidentiality and integrity are preserved throughout the process, then everything is good. The other end of the integration axis is a loose integration where the target company continues as an independent unit after the acquisition with some risk-based security hardening. This method changes the buyer's risk profile, and there should be ways to systematically map and deal with residual risk. This was the case in two companies whose CISO was interviewed for this research. They replaced the hardware and upgraded the network security from day one, giving the time needed for the rest of the integration.

The interviews revealed that there is no one-size-fits-all solution for risk treatment. It all depends on the integration plan. The only common denominator is a risk-based approach to security.

The last research question touched upon how much due diligence includes information security. The interviews revealed that those companies that acquire companies as their growth strategy do have a systematic track for cyber security. That includes security scans and applying threat intelligence techniques to find possible vulnerabilities. Quite often, there are findings that the target company was not aware of. The target company is typically asked to fix the vulnerability before closing the deal. If there are signs of exploitation of those vulnerabilities, that could mean cancellation of the deal. Some interviewees said that they have developed playbooks for the

information security track that use interviewing techniques to cross-check the collected documentation - and in a very constructive way.

The results from the interviews regarding how much information security was included in due diligence differed from the literature review that implicated a lack of information security tracks in due diligence. It would be interesting to do further research to find out when the trend has changed to its current state.

Could failures in M&A be avoided with better due diligence?

In the discussion on whether failures in M&A could be avoided with better due diligence, evidence suggests that enhancing the process could mitigate some common pitfalls. Interviews in this research indicate that more systematic due diligence approaches improve the success rate. This was an imminent statement from information security experts representing companies performing several M&A processes per year (30% of the interviewees). The target companies also appreciated their systematic approach since they received vital information security information about their own organisation.

This finding was also partly supported in the article “How companies got so good at M&A” from Harvard Business Review. “Acquiring companies gain experience and expertise by doing more deals. It’s no secret that the more often you do something, the more skilled you become. As organizations gain experience by making acquisitions more frequently, they learn what integration tasks they need to prioritise, what areas are likely to be troublesome, and how to make key decisions more efficiently.” (“A Better Approach to Mergers and Acquisitions,” 2024).

Neither information security nor systematic due diligence guarantees success in M&A. Five out of ten interviewees mentioned open communication and communication skills as important factors in the process. Subject matter specialists must communicate clearly and present the findings and possible deviations to the decision-makers.

A good way to avoid failures is to make smaller deals rather than complex megamergers. The interviews proved that companies can perform well through inorganic growth by acquiring smaller companies and merging them to the group.

Place for improvements in Due Diligence process

Many interviewees strongly suggested that ideally the information security function should be at least informed in the early stage about the M&A process to improve the process. Another clear improvement suggestion is that the questions placed to the target company should be clear enough, to make it easier to answer them.

The current status of CISO involvement varies depending on company's information security maturity level, industry, and organizational hierarchy and CISO's position in it.

Typically, the only information security-conscious decision maker involved in DD is CIO or equivalent ICT decision maker. That person, however, is not the same as the CISO responsible for information security. If this is the case, the CISO has to catch up overnight with the whole process and matters that have been going on for weeks or months. The extra workload is very heavy, since this is all an addition to the normal line work.

The positive news many interviewees mentioned is that CISOs are available for the process if asked.

6.2.1 Interpretation And Synthesis Of Results

This research studies Mergers and Acquisitions and Information security. The subject matter expert interviews revealed a lot of detailed information varying from high-level strategic matters to operational matters. The findings remain unclear unless a descriptive framework is produced as a synthesis. After several iterations of the numerous interview findings, the appropriate level of the abstract was reached, and it was introduced next.

Information Security Is a Dimension in Company Strategy

The Venkatraman Henderson (1990) Strategic Alignment model, heavily adjusted to information security, can be used to interpret the results and form a synthesis. This model was developed by the researcher because the research question of how CISO is involved in the M&A process raised another higher-level question during the research process: "Why is the CISO involved?" The interviews answered this question by analysing the M&A process with the RACI matrix. The answer

is quite simple: Information security is a significant dimension of business strategy, which is why CISO and the company information security function are needed in the process.

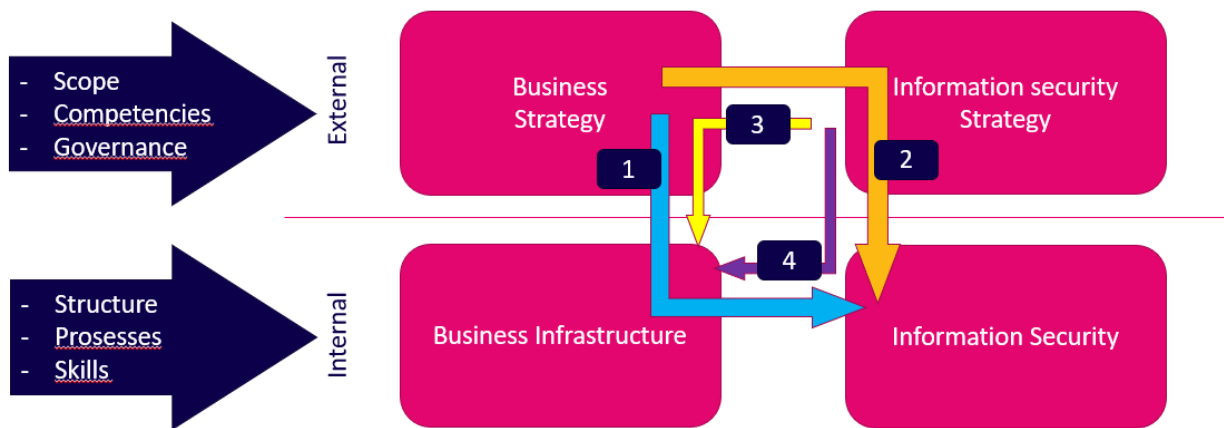


Figure 7: Information security alignment model.

The model is divided into two sections: external and internal. The external section on the top points to general business strategies and information security strategies' scope, competencies, and governance. The internal section on the bottom points to the organisational business infrastructure and information security's scope, which includes structure, processes, and skills. The arrows show four different approaches to this alignment model. The approaches are described in more detail later on.

Business Strategy and Business Infrastructure

The external business scope is, in other words, the markets, products, and business environment in which companies operate. Competency is typically competitive advantage and value creation to customers. Governance is the organisation structures and how businesses are organised, including outsourcing. Regulatory requirements also fall into this.

The internal business infrastructure consists of organisational structure, roles and reporting. Skills are the capabilities of employees to perform tasks. Also, motivation, training and company culture are vital for maintaining high performance and adaptability.

Information Security Strategy and Framework for Information Security

The external scope of information security strategy includes security frameworks like ISO/IEC 27001 and NIST, which provide guidelines and best practices for protecting information assets. Compliance with relevant laws and regulations, like GDPR, NIS2, and DORA, also falls into this scope. External threat models help identify potential security risks. There is a certain level of connection to ICT business strategies and technology models.

The internal information security scope includes a framework for information security or security to establish policies, procedures, and controls necessary to protect the company's information assets. Integrating information security into the development process is also within the scope for product security reasons. Finally, the workforce's information security and awareness skills and competencies need to be mentioned.

The Four Approaches

These four approaches are based on the idea that one of the external models acts as a starter and the other as a catalyst, based on which internal change is implemented.

Information Security Execution

Arrow #1 in Figure 7 typically refers to cases where business infrastructure is built based on business strategy but technical information security without a mature ISMS. Risks are not properly analysed, and the technical protection might be missing something. In some cases, information security is seen as an expense. Referring to the research interviews, this could be a typical scene in an SME or startup company.

Information Security Leverage

Arrow #2 in Figure 7 shows information security leverage where business strategy is the initiator and information security strategy is the catalyst. This is a typical M&A case where the buyer company implements a business strategy and applies information security strategy models for implementing the information security framework to the target company to make the target company compliant with the buying company with relevant policies, procedures and controls. This

approach demonstrates risk-based information security, where business outcomes are defined, and information security increases the success chances of these business outcomes.

Product Security

Arrow #3 in Figure 7 introduces product security. This is information security and privacy built into products or services. This differs significantly from the other approaches since this is not about organisational information security. Therefore, the traditional security workforce is not necessarily responsible for product security either. The starting point is information security models or regulation, like GDPR, DORA; HIPAA or relevant ISO/IEC standards that drive business strategies. In this research, the interviewees also discussed this by referring to secure software development.

Business Process Improvement

Arrow #4 in Figure 7 is initiated by information security strategy and applied to information security framework and business infrastructure. This is the improvement of processes or security controls based on threat intelligence or other changes from the external layer. This approach could also be applied to improving workforce skills with security and awareness training and digital skills

6.2.2 Ethical And Quality Discussion

This research follows the methods recognised in JAMK. The research work has been conducted with the highest possible care and precision. The recording and presentation of results are done with precision and honesty. The confidentiality of the information provided by the interviewees was maintained rigorously. Personal data collection has been minimal, and personal data has a clear retention policy that will be followed carefully.

The thematic analysis was conducted using a qualitative software tool, which facilitated the systematic categorization of data. The study acknowledged and addressed potential limitations. The methods contributed to the production of high-quality insights into the role of information security in mergers and acquisitions.

6.3 Conclusion

This study contributes to the theoretical understanding of the role of information security in M&As by highlighting the CISOs' and information security functions' roles and involvement in the process. It also suggests that organizations can improve the success rate of M&As by incorporating information security organizations or CISOs early in the due diligence process.

Future research

Future research should focus on quantitative research on the impact of early CISO involvement in M&A processes and exploring the effectiveness of the Information Security Alignment Model in various organizational contexts.

On other fields of research, the business culture, communication skills, and employee engagement in company's business transition would be interesting contribution too.

Epilogue

Ultimately, integrating information security practices into the mergers and acquisitions process is necessary. The digital landscape with consistently evolving threats requires organizations to prioritize information security at both the strategic and operational levels. Mergers and acquisitions are not the only events when the organization is subject to change and when information security must be reviewed. Organizational resilience must be kept at a high level at all times.

7 Acknowledgment

I would like to express my gratitude to the JAMK lecturers, especially Jari Hautamäki, whose guidance and feedback were valuable throughout this research.

I am also grateful to the Finnish cybersecurity community for its support, especially to the ten information security professionals who gave their time and shared their expertise for the interviews.

And last, the heartfelt thank you goes to my family and my parents, whose love, patience and support helped me reach this professional milestone – once again!

References

A Better Approach to Mergers and Acquisitions. (2024, May 1). *Harvard Business Review*.

<https://hbr.org/2024/05/a-better-approach-to-mergers-and-acquisitions>

Absalom, R. (2022a). *ISF Information Security in Merger and Acquisitions Briefing Paper*.

Absalom, R. (2022b). *ISF Security Challenges During Mergers and Acquisitions*.

<https://www.isflive.org/s/related-files?topicId=OTO6M0000005B8PWAU>

Athavaley, A., & Shepardson, D. (2017, February 21). Verizon, Yahoo agree to lowered \$4.48 billion deal following cyber attacks. *Reuters*. <https://www.reuters.com/article/idUSKBN1601EK/>

Benitez, J., Ray, G., & Henseler, J. (2018). Impact of information technology infrastructure flexibility on mergers and acquisitions. *MIS Quarterly*, 42(1), 25–44.

<https://doi.org/10.25300/MISQ/2018/13245>

Burke, D., & Kovala, S. (2017). ITMA - IT Integration in Mergers and Acquisitions. *International Journal of Business and Management*, 12(11), 16. <https://doi.org/10.5539/ijbm.v12n11p16>

Chui, B. S. (2011). A Risk Management Model for Merger and Acquisition. *International Journal of Engineering Business Management*, 3, 11. <https://doi.org/10.5772/50935>

Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document / READ online. (2015). Oecd-ilibrary.Org. https://read.oecd-ilibrary.org/science-and-technology/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en

Dunbar, J. K. (2014, September 1). The Leaders Who Make M&A Work. *Harvard Business Review*.

<https://hbr.org/2014/09/the-leaders-who-make-ma-work>

- Farrell, P. (2014, November 18). Mergers, Purchases Need Cybersecurity Due Diligence Survey Finds 78: Of Dealmakers Don't Eye That Risk. *Pittsburgh Post - Gazette*, E.5.
- Henderson, J. C., & Venkatraman, H. (1990). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, 38(2.3), 472–484.
<https://doi.org/10.1147/SJ.1999.5387096>
- Hepfer, M., & Powell, T. C. (2020). Make Cybersecurity a Strategic Asset. *MIT Sloan Management Review*, 62(Fall 2020).
- Junni, P., & Teerikangas, S. (2019, April 26). *Mergers and Acquisitions*. Oxford Research Encyclopedia of Business and Management.
<https://doi.org/10.1093/acrefore/9780190224851.013.15>
- Kantor, B. (2023, November 6). The RACI matrix: Your blueprint for project success. *CIO*.
<https://www.cio.com/article/287088/project-management-how-to-design-a-successful-raci-project-plan.html>
- Koskinen, I., Alasuutari, P., & Peltonen, T. (2005). *Laadulliset menetelmät kauppatieteissä*. Vastapaino.
- Larsen, M. (2005). *ICT integration in an M&A process*. 95.
- M&A integration and carve-out study*. (2023). Bearingpoint.
- Nash, K. S., & Minaya, E. (2018, March 5). Due Diligence on Cybersecurity Becomes Bigger Factor in M&A; Close scrutiny of tech operations can uncover cybersecurity gaps before deals close. *Wall Street Journal (Online)*, n/a.
- NIXU CyberSecurity Index Report 2023*. (2023). Nixu Oy.
https://www.nixu.com/sites/default/files/NIXU_CyberSecurity_Index_Report_2023.pdf?utm_campaign=2023%20Business%20Resilience&utm_medium=email&_hsmi=81293275&_hsenc=p2ANqtz-9lVVAMt2nFplzgoZNITpE4W4mKfnMqWzQ_HKHQ-

hbDCqs0VEja0pjHltsQOhScErmiQ7AUKL0UNukrhz9fU_-nVyY3KEVIqq-

tpoP2X_ZcEWuErPQ&utm_content=81293275&utm_source=hs_automation

Paananen, H. (2023). Information security policy development—Considering the practices of

making rules. *JYU Dissertations*. <https://jyx.jyu.fi/handle/123456789/85239>

Pearlson, K., & Huang, K. (2021). Design for Cybersecurity From the Start. *MIT Sloan Management*

Review. <https://sloanreview.mit.edu/article/design-for-cybersecurity-from-the-start/>

Porvari, P. (2012). *Tietoturvallisuus liiketoiminnan johtamisessa, prosesseissa ja henkilöiden*

toiminnassa [Doctoral dissertation]. Aalto University.

PRISMA 2020 flow diagram. (2024). PRISMA Statement. [https://www.prisma-](https://www.prisma-statement.org/prisma-2020-flow-diagram)

[statement.org/prisma-2020-flow-diagram](https://www.prisma-statement.org/prisma-2020-flow-diagram)

Rignell, J. (2019). *Yritysjohdon vastuu / tilivelvollisuus yrityksen kyberturvakysymyksissä*.

Kuvaileva/tutkiva tapaustutkimus kyberturva-asioiden vastuunjaosta [Aalto University

School of Business].

[https://aaltodoc.aalto.fi/bitstream/handle/123456789/42850/master_Rignell_Jere_2019.p](https://aaltodoc.aalto.fi/bitstream/handle/123456789/42850/master_Rignell_Jere_2019.pdf?sequence=1&isAllowed=y)

[df?sequence=1&isAllowed=y](https://aaltodoc.aalto.fi/bitstream/handle/123456789/42850/master_Rignell_Jere_2019.pdf?sequence=1&isAllowed=y)

Rosenquist, M. (2020, October 24). Cyber Risks During a Merger and Acquisition. *CISO MAG /*

Cyber Security Magazine. <https://cisomag.com/cyber-risks-during-merger-and-acquisition/>

Sadok, M., Alter, S., & Bednar, P. (2020). It is not my job: Exploring the disconnect between

corporate security policies and actual security practices in SMEs. *Information & Computer*

Security, 28(3), 467–483. <https://doi.org/10.1108/ICS-01-2019-0010>

Sherman, A. J. (2018). *Mergers and Acquisitions from A to Z* (4th ed.). Amacom.

[https://learning.oreilly.com/library/view/mergers-and-](https://learning.oreilly.com/library/view/mergers-and-acquisitions/9780814439036/xhtml/covers/cover.xhtml)

[acquisitions/9780814439036/xhtml/covers/cover.xhtml](https://learning.oreilly.com/library/view/mergers-and-acquisitions/9780814439036/xhtml/covers/cover.xhtml)

Sims, C. A., Sasha Cohen O’Connell, Iria Giuffrida, and Ronald R. (2023, December 20). *Adding Cybersecurity Expertise to Your Board*. MIT Sloan Management Review.

<https://sloanreview.mit.edu/article/adding-cybersecurity-expertise-to-your-board/>

Tervola, J. (2023, May 3). Yrityskaupassa it-yhteensopivuus pitää selvittää jo ennen kauppaa – jopa 90 prosenttia yrityskaupoista epäonnistuu. *TIVI*. <https://www.tivi.fi/uutiset/yrityskaupassa-it-yhteensopivuus-pitaa-selvittaa-jo-ennen-kauppaa-jopa-90-prosenttia-yrityskaupoista-epaonnistuu/a0548ce7-ac25-4783-8881-8941d99ffd56?ref=email:4880>

Tuomi, J., & Sarajärvi, A. (2019). *Laadullinen tutkimus ja sisällönanalyysi*. Tammi.

Vilkka, H. (2019). *Tutki ja kehitä*. PS-kustannus.

Wright, C., & Altimas, B. (2015). *Reviewing IT in due diligence: Are you buying an IT asset or liability?* IT Governance Publishing. <https://learning.oreilly.com/library/view/reviewing-it-in/9781849287210/xhtml/cover.html>

Appendices

Appendix 1. Interview Discussion Topics

Information security in M&A

Research Questions

Harri Hautala

jamk JAMKIN AMMATTIKORKEAKOULU
University of Applied Sciences

Interview anonymity, privacy, retention

- All interviews will be anonymous
- There is no intention to collect sensitive information
- Interview is recorded for transcription purposes and stored to researchers M365 account in JAMK.
- M365 account will be erased when studies end latest by end of July 2024

jamk

Interview structure

Qualitative research

- Topics:
 - Your background in this subject,
 - Due diligence process,
 - CISO involvement
 - ICT integration
- Keskustelurunko
 - Kerro taustastasi
 - Due Diligence prosessi
 - CISO/tietoturvahälytysten osallisuus
 - ICT integraatio
- Question throughout all topics:
 - Missing a vital point? What question should be asked?
- Kriittikki kysymyksiin sallittua:
 - Mikä kysymys olisi pitänyt esittää?
 - Mikä tärkeä asia tulisi nostaa esiin?

jamk

Topic 1: your background

- Tell about your background, roles and experience
 - M&A and Due Diligence
 - Information security

jamk

Topic 2: Due Diligence process

What is your experiences for the following?

- Phases of Due Diligence process
- How much does DD include information security audits?
 - What role does ICT have in general?
 - What parts (security governance, technical security) are included?
- What would be your suggestions for improving the DD process regarding ICT and information security?

jamk

Topic 3

Role of CISO (or infosec organization in general)

- Realistic
- Ideal

	Informed	Consulted	Responsible	Accountable
Initial Deal making				
Due diligence				
Pre-integration planning				
Integration				

jamk

Topic 4: Treating inherited system risk

- Treating legacy systems
 - Which risks?
 - Mitigation?
 - Residual risk treatment
- Treating Inherited procurement risk
 - Which risks?
 - Mitigation?
 - Residual risk treatment

jamk

Topic 5: ICT integration

How information security is taken into account in ICT integration process?

- What is your experiences?
- How and when is ISMS applied? Conversions from one to another
- Regulation challenges

jamk

Topic 6: side effects

- Malicious insider
- Key persons leaving for new jobs
- No key persons available / outsourced

jamk

Risk scenarios

Biggest risks

- Malware
- Ransomware
- Malicious insider
- Unintentional error

Planned	Very Likely				
Likelihood	Likely				
Possible					
Unlikely					
	Negligible	Moderate	Significant	Severe	
		Impact			



jamk

Appedix 2. RACI matrix

The four roles that stakeholders might play in any project include the following:

Responsible: People or stakeholders who do the work. They must complete the task or objective or make the decision. Several people can be jointly Responsible.

Accountable: Person or stakeholder who is the “owner” of the work. He or she must sign off or approve when the task, objective or decision is complete. This person must make sure that responsibilities are assigned in the matrix for all related activities. Success requires that there is only one person Accountable, which means that “the buck stops there.”

Consulted: People or stakeholders who need to give input before the work can be done and signed-off on. These people are “in the loop” and active participants.

Informed: People or stakeholders who need to be kept “in the picture.” They need updates on progress or decisions, but they do not need to be formally consulted, nor do they contribute directly to the task or decision.

(Kantor, 2023)