jamk

How Situated Organizational Information Security Practices Emerge in Subsidiary Companies

A Case Study

Joni Koivuaho

Master's thesis
May 2025
Master's Degree Programme in Information Technology, Cyber Security

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Koivuaho Joni

How Situated Organizational Information Security Practices Emerge in Subsidiary Companies, A Case Study

Jyväskylä: Jamk University of Applied Sciences, May 2025, 58 pages

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

Permission for open access publication: Yes

Language of publication: English

Abstract

The information security of subsidiaries has been studied little, if at all. This is surprising, considering that subsidiaries are a common form of business. This study examines the information security practices of subsidiaries and their development.
A qualitative exploratory case study was conducted to examine the impact of various factors, such as organizational structure and institutional pressures, on the development of information security practices in subsidiaries.
The case study is an organization operating in Finland that is a subsidiary of a European company operating in several European countries. The study was conducted in one phase between February and May 2025. The study used documentation from the case organization as material, and additional data was obtained through semi-structured interviews and participatory observation.
The study found that organizational structure has a strong influence on the formation of information security practices. It was also found that institutional pressures do not affect subsidiaries as much as independent companies in the formation of information security practices.
Information security in subsidiaries is an area of research offering new and exciting opportunities for researchers interested in organizational information security. The topic is also becoming increasingly relevant.

Keywords/tags (subjects)

cyber security, cyber defence, data security

Miscellaneous (Confidential information)

-

Contents

Figures

Tables

1 Introduction

1.1 Overview

Information technology significantly improves the effectiveness of governments and businesses and the quality of life of individuals, but the cyber environment also poses significant security threats to all of them (Carr et al., 2021). In general, information technology has enormous social importance, and the security of information systems is the foundation of personal security, the protection of fundamental rights and the "trust and dynamism" of the economy, society and democracy (European Parliamentary Research Service, 2020). As critical societal functions, such as security and the economy, are increasingly based on or dependent upon information technology, they are also increasingly being operated by the private sector companies (Newlove-Eriksson et al., 2018). In recent years, the number of new types of information security threats has increased, and the consequences of information security incidents have become almost an everyday occurrence. This is a study of how private companies prepare to defend themselves, and indirectly greater society, against information security threats.

The purpose of this study is to increase understanding of how information security practices are formed in organizations, and how circumstances such as the operating environment or organizational structure, and changes therein, or institutional pressures influence choices in the formation of situated information security practices. For this study, I chose the perspective of a subsidiary. In literature, organizational information security has generally been studied in the context of independent and autonomous entities. However, subsidiaries that are operationally dependent on and controlled by their parent companies are becoming more prevalent. For example, In Finland, foreign-owned companies control more than a third of the country's €430 billion in corporate assets (Luoma, 2021), and although no straightforward conclusion can be drawn from the number of, the majority of these undoubtedly are subsidiaries. The relationship between subsidiaries and their parent companies has not been widely studied from a non-financial perspective, and much less an information security perspective.

The research interest of this study is the formation of information security practices in subsidiaries. I am investigating this phenomenon in a case organization operating in the business process

outsourcing industry in Finland, which is a subsidiary of a European company operating in several European countries. The study was conducted in one phase between February and May 2025.

1.2 Research Background

As a novice researcher, information security seems to me to be a very broad concept and a rich source of research opportunities. In recent years, there has been extensive research into information security, both in academia and by various professional services firms. As a professional, I am interested in organizational events and phenomena, especially those at the intersection of operations and technology, as well as their causes and consequences. This interest turned into a thesis on information security practices within the organization.

When planning this thesis and drafting its topic, I came across a conflict between literature and my own everyday experience as an information technology consultant. In the academic literature on information security, organizations are always examined as self-contained, decision-making entities. This is natural, given that science seeks to generalize, and most organizations are still traditional independent companies. Today, however, more and more people work for companies where the company's real decision-making power is limited due to its status as a subsidiary. The group headquarters is often the place where decisions concerning IT systems, processes, and security are made. At the same time, however, information security is considered a function whose practices should be developed based on local conditions and risks. This interesting contradiction led me to investigate the topic further.

Subsidiaries have been studied regularly in business management journals as well as economics and finance journals. Most of this research focuses on financial aspects, but there are also some studies that examine the operational aspects of the subsidiary's position. These operational studies have examined, for example, mechanisms by which parent companies control subsidiaries, or how subsidiaries implement the policies of their parent companies. These studies have often applied established and strong theories originating in the social sciences, which has led to insightful research and produced important new information. The study by Kostova and Kendall (2002) is an excellent example of this. In their study, which covers over a hundred subsidiary companies, they used institutional theory to examine the mechanisms by which practices are transferred to subsid-

iaries in multinational companies and how this happens. Similar theories, such as institutional theory, have also been widely used in the field of information systems. This is natural, as organizational research and information systems largely share the same subjects of interest, only with different perspectives. Given that general theories and research results are already emerging in other fields, it would be natural to apply the same research approach to information security.

1.3 Organizational Information Security as a Research Topic

This study draws considerably on research in information systems. Information systems can be considered the parent discipline of organizational information security research, which distinguishes it from most technical information security research, which has its origins in computer science (Björck, 2004; Paananen et al., 2020). Other disciplines closely related to information technology, such as computer science, focus on the technology itself, but the information systems is a discipline that focuses on the development, use and impact of information technology in organizations (Myers & Avison, 2002). However, it should be noted that information security research as part of information system science is still relatively young and continues to seek its strong research directions whereas computer science has produced vast amounts of research in the information security field (Rea & Marshall, 2020).

To begin this thesis, I conducted a literature review, basing it on Levy and Ellis (2016) and broadly following their guidelines on keyword search, backward and forward search, quality of research literature, and applicability of literature to my thesis. During the literature review, my goal was to identify and understand the current areas of interest in organizational information security, particularly within information systems research, e.g., what theories have been proposed, and where there are potential research gaps and needs for further research. My main sources for the literature review were three databases: Scopus, Web of Science, and IEEE Xplore Digital Library. I preferred leading peer-reviewed information systems journals, such as the ones in the Association for Information Systems' Senior Scholar's List of Premier Journals, as well as journals in the information security field such as the Journal of Information Systems Security and Computers & Security. I have also examined conference proceedings in the field of information systems. Later, as my knowledge grew and I wanted to gain a deeper understanding, I expanded my research to include original articles from organizational research and social sciences, as information systems research often borrows from these.

The increased importance of information security in the everyday life of organizations is now reflected in the rise of research on management of information security. For example, Signh et al. (2023) identified management of information security as one of the five key academic research trends in information security in their bibliometric citation analysis. According to Malatji et al. (2020), a more holistic, i.e., an organizational or governance-centric, approach to information security is important because "taking overly technocentric approaches to enterprise security risk does not yield significantly positive results in protecting assets". The same has already been argued by Soomro et al. (2016), who in their systematic literature review found that management actions in particular have an impact on information security, and therefore suggested a more holistic approach to information security rather than it being just the technological context. However, this shift towards more holistic information security approach has historically been quite slow.

In information systems, the research community began discussing as early as the 1980s that technology is only one part of larger information system and that this should be taken into account in research, development and implementation in the field (Myers & Avison, 2002). In information security research, the same kind of thinking began to emerge about 15-20 years later. Dhillon and Backhouse (2001) discussed the tradition of information security research, noting that it had been largely focused on technical-mechanical solutions in simplified, hierarchical, organizational settings. However, according to them, as networked organizations and technology interactions with realities outside the organization have made information security a strategic issue, research should focus more on the organization and social reality.

Similar arguments can be found in von Solms and von Solms (2004) in their identification of the 10 deadly sins of information security. Perhaps more importantly, by deadly sins they demonstrate the fundamental nature of information security as an operational, socio-technical, and multidimensional issue. The article was a natural progression from von Solms' earlier research (2001), which noted that information technology and information security are becoming increasingly important to organizations, and that the impacts need to be integrated into corporate governance and risk management. In the past, information security has been viewed as a technical issue and therefore solutions have naturally been technical as well (Singh et al., 2013).

Organizational information security has now been a subject of broader interest to researchers for 25 years. It has also been studied from different viewpoints, and different periods can be distinguished based on the specific focus of the research. Initially, the focus was purely on behavior and the secure use of information technology, strongly based on the idea that "the user is the weakest link in information security". Organizational behavior information security research has examined topics such as how individual users should behave to prevent information security breaches, how to identify potential information security breaches, and how to respond when an information security breach is detected (Cram et al., 2017). Eventually, in the late 2000s the research agenda expanded to include information security policy, mainly in terms of how secure behavior and the use of information technology should be directed in organizations.

However, this research on individual user behavior left out or largely buried an interesting and equally important aspect of the formation, implementation and effectiveness of organizational information security practices (Cram et al., 2017). Straub et al. (2008) suggested that a key question in information security may be how organizations decide where their information security needs are, and how they organize information security practices accordingly. Similar idea had already been argued by von Solms and von Solms (2004), who framed the questions that an information security responsible in organization should be able to answer: "Against which risks must the information resources be protected?" and "What set of countermeasures will provide the best protection against these risks?".

1.4 Organization's Goals lie at the Intersection of Risk Management and Trust

In the first decade of the 21st century, information security regulations were still in their nascent stages, and IT departments were primarily responsible for systems while also being responsible for keeping attackers out on a part-time basis (Andress & Leary, 2017). With the spread of information technology within organizations, its implementation is no longer the sole responsibility of technical professionals. And what has happened to information technology in general has also happened to information security. As Bruce Schneider aptly stated (2017), "As everything turns into a computer, computer security becomes everything security".

In today's news environment, it would be intuitive to say that improving information security and its management is probably on every organization's agenda for the good of the business, but in a

world of limited resources, information security may not always be at the top of the priority list. In an ideal world, security would be seen as a direct strategic investment or competitive factor, but in reality, placing security at the center, or even as part of the strategy, has proven challenging. Instead, in today's networked operating environment, information security is undoubtedly natural part of good corporate governance (De Bruin & von Solms, 2016), corporate social responsibility (Harkins, 2016; Khan et al., 2025) and, at the same time, an increasingly important part of an organization's trust capital. Wider society – which may include customers, employees, business partners, and the government – expects organizations to handle and store information responsibly, secure their environments, and act responsibly and transparently in the event of an incident.

There are numerous reasons related to good corporate governance that may require an organization to take action to improve its information security posture. For example, an organization's stakeholder may require that the organization's information security is properly managed before establishing or retaining a stakeholder relationship. Senior management's commitment to information security has increased significantly due to the acceleration of regulation, and serious consequences can result from failure to comply with regulatory requirements (Ransbotham & Mitra, 2009). In Western countries, broader information security regulation first began in the United states in the early 2000s in the financial sector with the recognition of the importance of information security in the Sarbanes-Oxley Act, and the European Union has accelerated regulation since the mid-2010s with, for example, the NIS and GDPR directives. (Ransbotham & Mitra, 2009)

When information security is a key component of good corporate governance and enables social responsibility, it naturally generates also broader well-being and is clearly part of the sustainable development that our society aims to maintain. While information security is not explicitly included in the United Nations Sustainable Development Goals (United Nations, n.d.), it contributes to or facilitate those goals. Information security is a key component of SDG9 – *Building resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation* – and SDG16 – *Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels*.

Today, information security practices in organizations are quite strictly regulated. These regulations establish minimum standards for specific industries and are designed to protect the trust

that customers and other stakeholders expect from organizations operating in those industries. However, compliance with these requirements should not replace information security practices based on genuine risk management needs, not it should never be the primary objective of organization. (Andress & Leary, 2017)

Although compliance with regulations should not be a company's primary objective, building internal and external trust by promoting good governance and social responsibility, and implementing appropriate risk management should definitely be primary objective of organization's information security function. This objective is not in conflict with the main objectives of other organizational functions.

Hsu et al. (2012) stated that information security management is primarily an administrative rather than a technological innovation. Therefore, information security management cannot be separated from institutional pressures or other similar factors that affect an organization anyway. Cavusoglu et al. (2015) studied different kinds of institutional pressures that organizations experience regarding their information security and improving it. They found that institutional pressures significantly explain why organizations devote different amounts and different resources to information security controls, and thus why security practices differ between organizations, even when business models are very similar.

1.5 Research Questions and Study Design

Von Solms and von Solms (2004) pointed out that most of the threats, risks, and countermeasures relevant to information security are typically common to all organizations. This is why organization should build on the experience of others, rather than "reinventing the information security wheel". They noted that this valuable experience has been captured in internationally accepted standards that usually represent the consensus view of experts in information security.

Over the last thirty years, numerous information security management standards, such as ISO/IEC 27001, have emerged by government authorities, internal treaties, and private sector actors. In addition to bringing together experience from the field, these standards can be seen to provide a common set of concepts and controls for practitioners implementing security practices across the organizations (Bouraffa & Hui, 2025). And in general, information security management standards

have proven to be an effective overall guidance for organizing information security in many respects (Smith et al., 2010). While these standards have become more widely recognized, the institutional pressures to implement them to strengthen an organization's information security posture have increased (Cavusoglu et al., 2015).

These information security management standards have also been criticized. Although von Solms and von Solms stated (2004) the age-old truth that information security management is about doing the right things right, the information security management standards, such as ISO/IEC 27001, focus primarily or exclusively on the right way to do things, or in other words, on the process (Siponen, 2006). If we pay attention to how and for what purpose these standards have been created, we quickly realize that they have been created by generalizing the field knowledge into very universal form of guidance (Siponen & Willison, 2009). And because of their nature, they tend to focus more on specific artefacts than on the practical realities of the organization, which means that even if the standard is fully implemented, the real objectives of the organization may not be achieved (Siponen, 2006).

Building on previous research on information security management, Niemimaa and Niemimaa (2017) pointed out a research gap in how contextualization of these universal and generalized standards, such as ISO/IEC 27001, has been implemented in different organizations. This contextualization process aims to translate the general guidelines into an organization's localized information security management system, i.e., information security policies and technical security controls. They did their ethnographic study by observing how a given standard requirement was translated into a localized policy in an anonymized IT service provider. This study was to increase the understanding of the practical work and problems of information security management in an organization.

In addition, Niemimaa and Niemimaa (2017) combined previous research on information security management with the theory of canonical and non-canonical practices in organizations by organizational theorists Brown and Duguid (1991). In their original article, Brown and Duguid underlined the difference between formal guidelines and actual work. They called formal guidelines canonical practices, and in contrast, they called actual work and tacit knowledge as non-canonical practices. Niemimaa and Niemimaa (2017) used the concepts of canonical and non-canonical practices and

intuitively linked them to organizational information security in the sense that there is a similar tension between external information security management standards, such as ISO/IEC 27001, and organizations situated information security practices.

The process that leads to the localization of these formal, rather general, guidelines into situated practices is called translation. The translation is a theoretical concept originally introduced in sociology, but since then it has also been introduced in organizational research (Czarniawska & Joerges, 1996; Wæraas & Nielsen, 2016). The theoretical concept of translation "surpasses the linguistic interpretation" in the sense that it can involve interpretation, but especially in the sense that it always involves some kind of reformulation of an idea to fit the target context (Czarniawska & Joerges, 1996), which makes the concept quite useful in the case situated information security practices as well.

This thesis continues the work begun by Niemimaa and Niemimaa and aims to increase the understanding of the everyday nature of information security in organizations and to reveal the mechanisms that lead to the localization and emergence of information security practices in organizations, this time from the perspective of a subsidiary company.

Eventually, the actual research question became clear:

- How have the internal, situated, information security practices constructed in a subsidiary company?

To obtain a comprehensive understanding, I identified the following sub-questions:

1. What are the localized information security practices?
2. What material factors have affected the localization?
3. What non-material or social factors have affected to the localization?

The design of the study is presented in Figure 1. The case organization, its unique or distinctive characteristics, and the environment in which it operates are described in Chapter 4. The sub-questions are addressed in Chapter 5, which describes the current information security practices of the case organization and establishes a basis for the second and third sub-questions. The sec-

ond sub-question aims to identify the essential factors that influence or have influenced information security arrangements, such as organizational structure or IT systems. The main source of information for these research questions is the organization's internal documentation.

The third research question aims to identify the intangible, tacit, and social factors that influence or have influenced the information security practices of the target organization. These factors include various institutional pressures, such as mimetic or normative pressures. The source data related to the third subquestion is tacit in nature and would require strong interpretation if documentation were the only source of information. To avoid an error-prone and risky interpretation process, the third subquestion is not answered based solely on documentary sources. Instead, information was collected from the organization through semi-structured interviews.

Chapter 5 aims to lay the groundwork for answering the study's main research question, which is examined in more detail in Chapter 6. Chapter 6 contains conclusions and a discussion that comprehensively address how a subsidiary's position affects information security practices.

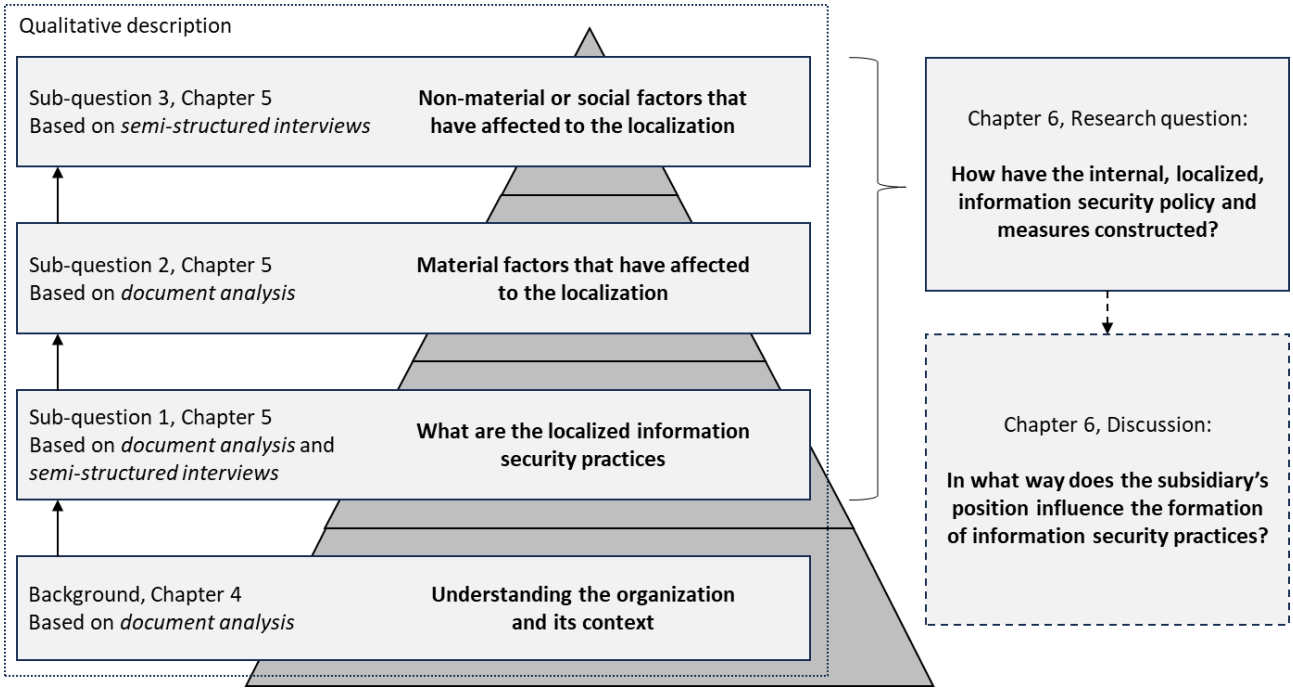

Figure 1. Study Design

2 Theoretical Framework

As a part of the literature review, I have found a number of broader theoretical backgrounds that relate to the topic of this study. The initial aim of the search was to identify the theoretical foundations that have already been used in the studies of information systems or information security research. A key criterion for searching was that these theories could be used in some way to explain the formation and development of information security practices in organizations. Another key criterion was that the unit of analysis be an organization, meaning that the theory can explain specific events within an organization rather than broader societal changes or the behavior of individuals or groups. The two theories that I have identified as particularly relevant to this thesis are *contingency theory* and *institutional theory*.

2.1 Basic Concepts of Information Security

Before going into the actual theories, it is useful to familiarize oneself with some basic concepts that I will be using in this study. In my initial literature review, I found that some terms I was already familiar with were not universally and consistently used in the literature. I also found that some of these terms were specific to certain periods, trends and theories of research. Similarly, I found that some concepts commonly used in the industry, for example, those used in ISO/IEC 27001 standard, are not widely used in academic literature. In this section, I clarify the key concepts that are used in this thesis, how these concepts should be understood in the context of this thesis, and how these concepts should be related to others found in literature.

This thesis belongs to the field of *information security*. Andress and Leary (2017) explain information security in everyday language: “In essence, it means we want to protect our data and the systems that hold it form those who would seek to misuse it.” Based on the literature review, information security is used more than *cybersecurity* or *cyber security* in academic literature. “These terms are commonly used interchangeably” (Taherdoost, 2022), but they have tone differences depending on the perspective used. In the information systems field, some studies have called this whole as *Information Systems Security* (for example, Burgurcu et al., 2010) or *IS Security*. There is a fairly broad consensus in the security literature on the meaning of information security: it is about ensuring the confidentiality, integrity and availability of information (Lundgren & Möller, 2019), although this definition is occasionally challenged (for example, Lundgren & Möller, 2019). What is

more controversial are other aspects of the definition, such as its scope. The most common view is that cybersecurity is a subset of information security, with cybersecurity covering security of information in cyberspace, while information security covers, in addition to that, for example, physically stored data (Taherdoost, 2022). This is the definition of the term that I use in this study.

The organization is fully responsible for managing a secure information and IT environment and for the secure processing of data. For this purpose, the organization manages its technical and human resources and processes in such a way that the company's internal and external information security requirements can be met (Ransbotham & Mitra, 2009). The established practices that an organization uses to prepare for or respond to information security threats can be referred to as organization's *information security practices*.

There are many names for the formal structure used to manage an organization's information security practices. Some studies in the field of information systems research refer to this whole as an *information security system* (Bouraffa & Hui, 2025), *information security program* (Knapp & Ferrante, 2014) or *cybersecurity program* (Büyüközkan & Güler, 2025), *organizational security program* (Knapp et al., 2009), or *information security process* (Straub et al., 2008). In the field of information systems, even in highly cited papers, this concept has not been clearly defined. The International Organization for Standardization uses the term i*nformation security management system* or *ISMS* for this concept and defines (n.d.) it as "part of an overall management system, based on a business risk approach, that creates, implements, operates, monitors, reviews, maintains and improves information security". In this study, the term information security management system is used.

In the field of information systems and organizational information security in general, the highest-level security policy document of an organization is referred to as the *information security policy* or *ISP*. In this study, the term information security policy is used to express the organization's objectives with regard to information security. This document may also contain directives on practices to reach these objectives, or these may be sub-documents of the ISP. It should be noted that older versions of the ISO/IEC 27001 standard required that the organization's highest-level policy document be referred to as *ISMS policy*. This refers to the same document, and the name of the required document has since been changed to *Information security policy*. The literature refers to

other documents of a similar nature. For example, National Institute of Standards and Technology (n.d.) defines an *information security program plan* as a document "that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements".

2.2 Contingency Theory

The *contingency theory* originated in the organizational research of 1950s. Contingency theory is based on the finding that there is no single "best way to organize" because organizations' internal and external conditions vary (Weill & Olson, 1989). Another key finding underlying contingency theory was that it still does matter how to organize as different ways of organizing vary in their effectiveness. (Reinking, 2012)

Contingency theory can be seen as focusing on the internal organizational structure and variables, such as types and sizes of organizational subunits, tasks, technologies, and personnel, and the entirety of these in relation to each other and the environmental conditions; under different conditions, these variables or their relationships must be altered (Bouraffa & Hui, 2025).

In organizational research, theory has been used to explain organizational forms that correspond to specific circumstances. In contract, in the field of information systems, theory has traditionally been used to design information systems that take organizational variables into account. This study does not directly apply contingency theory as it is commonly used to find a suitable way to organize internal operations. Instead, it uses contingency theory as an underlying truth. According to this truth, an organizations cannot be isolated from their environments and must adapt their internal structures and practices to their circumstances. In practice, this truth must be taken into account, for example, when applying norms, standards and guidelines.

2.3 Institutional Theory

The *institutional theory*, also called as institutional logic, has already become a robust perspective in information systems research (Nielsen et al., 2014). It has roots in sociology and organizational

research. The basic idea of institutional theory is to shift thinking from an economic-rational perspective to something deeper about the social situations, practices, or pressures that an organization faces and that affect its functioning, and this perspective can help to understand, for example, "how legitimate social facts are socially constructed and what consequences they bring about" (Currie, 2011).

As contingency theory, institutional theory research also often takes the organization as its unit of analysis. Institutional theory emphasizes social and cultural factors, therefore also external norms and values, shape the internal world of organization (Cavusoglu et al., 2015). The use of institutional theory, which to some extent, has become mainstream in information systems research, could respond to the need to research information security as a deeper organizational phenomenon and also provide an appropriate theoretical background for this thesis.

Understanding a few basic concepts commonly used in institutional theory is useful for understanding its logic. The study by Cavusoglu et al. (2015) can be used for this purpose. They examined the various external pressures organizations face regarding information security:

- Industry and competitors create *mimetic pressure*, which usually leads to the copying of methods or processes.
- *Coercive pressure* occurs when other organizations or authorities pressure an organization to adopt specific methods or processes.
- *Normative pressure* derives from what is considered good practice in an industry and from a desire to belong to a group.

Institutional theory is central to this study because, although the risk-based security needs arise within organization, institutional pressures, according to theory, guide actions, such as the choice of practices. Therefore, to answer the questions about how situated information security practices emerge, it is necessary to understand the institutional influences and pressures organizations face.

2.4 Usage of Theory in This Study

This study focuses on a topic that information systems or security researchers have not studied in the past for one reason or another. Perhaps the security arrangements of subsidiaries has not

been studied because practitioners, who don't use scientific journals as a primary information source, are better informed about these issues than researchers. It may also be that the topic is not considered significant by researchers. It may also be considered merely a special case of general principles, which researchers find uninteresting. Alternatively, it may not have been studied because the subsidiaries as a topic is closer to management research, with which information security researchers are less familiar. In any case, the topic is not well known in scientific literature.

When examining topics that have received little attention in previous research, it is rare to find any existing theory-based hypotheses available. It is also the case in this study. To gain an initial understanding of the phenomenon, it is necessary to study the topic comprehensively. Hopefully this will lead to generalizations or theorizing at a later stage. In this study, I accept the fact that a useful description of the phenomenon is sufficient new knowledge.

In this study, two theories, contingency theory and institutional theory, are used as a lens through which to view the findings that emerge from the data. In other words, unlike deductive reasoning, where hypotheses are derived from theory and tested with data, this study uses theory as in later stages of research to explore and structure themes that emerge form the selected and collected data. The material is therefore first analyzed before using the theoretical lens. In this context, the analysis of the material refers to classification, which facilitates thinking of the possibilities for new generalization and theorization through the existing theory.

3 Implementation of a Study

The goal is to describe the object of the study, the phenomenon, in a straightforward manner. So, this is a descriptive study. The intention is to provide a thorough description of the phenomenon in everyday language. This is accomplished through a research design that combines data acquisition, analysis and presentation methods in a sensible way. The selected methods provide a clear description of the phenomenon.

The research data was obtained by accessing organization's information security documentation. From this documentation, I selected key material essential to understanding the phenomenon. As research progressed, I categorized the topics raised in these documents and obtained additional information through semi-structured interviews, direct questions, and participatory observation.

Data was later analyzed and presented using a method called qualitative description. The variety of qualitative methods, their characteristics, and their applications initially caused considerable confusion for novice researcher I am. The practical nature of information systems also pushed me away from too interpretive methods. However, qualitative description, the basic form of qualitative research, is a recommended method for novice researchers learning qualitative research and for those investigating practical phenomena. Qualitative description differs from many other qualitative methods in that it focuses on practical questions such as who, what, and where. It aims to answer the question of why without strong interpretation, overly theoretical reflection, or redefinition of the context. Qualitative description also offers methodological flexibility, and as so, it allows researchers to use different theoretical lenses quite freely. (Hall & Liebenberg, 2024)

3.1 Nature of the Phenomenon Under Study

The research strategy and methodology used in this study were selected based on the phenomenon being studied, available data, and the data that could be collected. Another important factor in choosing the strategy was the ontological and epistemological aspects of the topic. These aspects arose from the nature of the phenomenon being studied and also from my own preconceptions about it.

Information systems science is focused on IT artefacts, including their characteristics, design, construction, implementation, use, maintenance, further development, and the ways in which they influence and are influenced by their contexts (Benbasat & Zmud, 2003). The phenomenon examined in this study is the formation of situated information security practices in organizations. As noted earlier, this is a common yet context-specific organizational dynamic and socio-technical phenomenon. Since its context-specific nature, I decided to study it empirically in its natural environment. Its dynamic nature, the historical development and continuous change of an occurrence, guided me to try to understand the phenomenon as a contextual process. In accordance with the research tradition of information systems, the focus is on the socio-technical rather than technical aspects. The unit of analysis is the organization, rather than the individual or society. Based on the socio-technical nature of the phenomenon, the objective of the research is to reveal the state and developments of the specific instance – the information security practices of the case organization, and through this, understand the phenomenon as a whole and potentially its causal mechanisms.

3.2 Case Study as a Research Strategy

Case studies are the most common research strategy among qualitative researchers (Rashid et al., 2019). Case studies are also the most common qualitative research strategy in the field of information systems (Myers, and David E. Avison, 2002). It quickly became clear that also I would examine this phenomenon as a case study. A case study is a research approach in which empirical data is collected from a natural setting to analyze a contemporary phenomenon (Myers & Avison, 2002). Or as Crowe et al. (2011) put it: “A case study is a research approach that is used to generate an in-depth, multi-faceted understanding of a complex issue in its real-life context.” The strength of case studies lies in the insights they provide because of their depth, which come from taking a specific case and delving deeply into the real-world context (Simons, 2014). In general, a case study can be thought of as a research strategy which is not tied to a particular perspective or methodology (Simons, 2014).

The case study as a research approach emerged in the social sciences in the 20th century. Modern anthropology has its roots in the ethnographic field observations conducted by Bronislaw Mali-

nowski among remote Pacific tribes. Case studies were a qualitative research method based heavily on fieldwork. This same approach was later adopted in French and American sociology, especially the so-called Chicago School of Sociology. (Hamel et al., 1993)

Today, case studies are not viewed as solely a qualitative approach. In fact, “there is no consensus on the basic characteristics of case studies”. Rather, the nature of the problem being studied combined with the paradigm settings determines how a case study is viewed. Positivists seek more hypothesis testing and verification from case studies and often base their research on quantitative methods. On the other hand, naturalists seek to generate new knowledge and enable theory formation through case studies by exploring uncharted areas using qualitative methods. The third type are the constructivists, who seek to advance existing theories by testing and developing them through new case studies. (Blatter, 2008)

Today, the prevailing view is that naturalistic case studies are, in many respects, a perquisite for theory formation (Benbasat et al., 2002). In other words, theory formation in many cases requires first qualitative case studies and in-depth analysis of the social reality of the case. As stated earlier, the role of information security in subsidiaries has not been studied in depth. In order to understand the phenomenon sufficiently enough, a naturalistic, exploratory approach is required. Furthermore, the nature of the available research data is such that only with qualitative methods can produce appropriate results for this study. For these reasons, this study employs a naturalistic qualitative case study approach.

Ketokivi and Choi (2014) underline the importance of the implementation of duality criterion for the success of case studies. That is, to be successful case study, the study should be grounded in the local situation and at the same time provide some general information about the research topic, meaning the aim for generalizability.

Generalization is the use of individual observations to create concepts that help us understand a broader reality. The goal is to establish clarity and order. These concepts are useful for understanding future cases, and eventually, a theory may be built around them. It is important to note that the concepts, not the content or context of the case, are generalized. (Simons, 2014)

Thomas (2011) argued the same: a case study should consist of two elements: a subject and an object. The object, the phenomenon, is the focus of the study that the case opens up or explains. The subject, or the case, is what gives access to the object. As previously stated, the object of this study is “the formation of information security practices”, and the subject is the case organization.

It is important to note that this division between subject and object is important for the formation of new knowledge and theory. This examination through a general theoretical background or lens distinguishes a scientific case study from a travelogue, because a report of an event does not in itself constitute a scientific case study. (Mitchell, 2009)

Case study should always aim to create new knowledge. From this point of view, a critical requirement for a case study is that some contextual data is used during and as input for scientific reasoning. Scientific reasoning has traditionally been considered to include inductive and deductive reasoning, but as Niiniluoto shows in his article (1999), abductive reasoning should also be included, regardless of the discipline. In a well designed case study, both the reasoning and the resulting claims or theory should be presented in a clear and transparent way so that these claims or theory and their logical consistency and overall validity can be evaluated. (Ketokivi & Choi, 2014)

3.3 Data Collection

Since the objective of qualitative case studies is to provide a rich description of a single phenomenon or organization, documents are typical and applicable data source for case studies (Bowen, 2009). This study uses existing documentation, policies, minutes of meeting, and other background materials, as the main data source.

As qualitative researchers aim to get as close as possible to the subject of their research in case studies, documentary sources must be supplemented with other data sources. This process, known as triangulation, aims to supplement the picture of the case formed from the documents. In addition to documents, these sources may also include, for example, interviews, which are used in this thesis to complete the overall view provided by the documents, to confirm conclusions and to reduce the number of conclusions that could erroneously be drawn from the documents alone. (Bowen, 2009)

In this study, semi-structured interviews have been used to gain initial understanding, and as part of each research phase and topic to provide a more detailed description and understanding of the topic. Additionally, I worked within the organization during the research period. Therefore, the document analysis and semi-structured interviews were supplemented by my participatory observations.

3.4 Description of Data Collected

I began collecting data by conducting a one-hour semi-structured interview with the IT leadership of the case organization. The purpose of the interview was to gain an overview of the organization's information security practices. I outlined preliminary interview themes, including information security governance, risk management, technical security measures, event monitoring, and incident management. Based on the interview and other material, I later refined these themes. More information on confirmed themes can be found in Chapter 5.

The case organization enabled my study by providing me with access to its written norms. I selected 33 documents for further analysis. These documents are information security policies or related to information security some way. These documents are highly interconnected in that they refer to each other. These documents are the core of the data base for this study. These documents are listed in Table 1.

In addition to the written norm, I was provided with typical IT documentation, including for example application architecture. On the business side, I had access to the company's process descriptions. In terms of information security documentation, I was granted access to hundreds of documents, including for example security controls and penetration test reports. However, for further analysis, I selected only those documents that were necessary for a better understanding of the research object itself. I also conducted separate interviews with the IT director, the Regional Information Security Officer, and the Risk Manager. Each interview lasted one hour. The purpose of the interviews was to validate my observations and ensure that I understood everything correctly.

Table 1. Information Security Related Written Norms of the Case Organization

Information Security (IS)	**ICT**	**Risk Management**	**Data Protection**
Information Security Policy	ICT Procurement Policy	Business Continuity Mgmt. Policy	Data Protection Policy
(*redacted)	Asset Mgmt. Policy	IS Risk Mgmt. Policy	Data Retention Policy
Clean Desk Policy		Outsourcing Risk Policy	Data Breach Policy
Physical Access Policy		Emergency Plan	Code of Conduct
Super User Policy		Risk Mgmt. Procedure	Data Governance Policy
Access Mgmt. Policy		Procurement Policy	Master Data Mgmt. Policy
Data Mgmt. Policy			(*redacted)
Incident Mgmt. Policy			Document Archiving Policy
3rd Party Policy			
Email and Internet Usage Policy			
SW and HW Usage Policy			
BYOD Policy			
Security Architecture Policy			
Security Development Policy			
Security Monitoring Policy			
Security Maintenance Policy			
Business Continuity Policy			
Total 17	2	6	8

** Redacted to protect the case organization's anonymity*

3.5 Data Analysis Method

I understand qualitative research as an approach in which qualitative data is systematically analyzed to achieve an in-depth understanding of a phenomenon. Objective of this is that the details in real life context can reveal something about the whole that is not directly expressed anywhere. Ketokivi and Choi (2014) make a clear distinction between qualitative and quantitative research by using the original meaning of the words qualitative and quantitative. According to their statement, the quantitative research is an approach that "examines concepts in terms of amount, intensity, or frequency", and qualitative research is an approach that "examines concepts in terms of their meaning and interpretation in specific contexts of inquiry".

The most important source data for this study consist of the case organization's policies and other documents. I have analyzed the content of these documents, and in later chapters I describe my findings. This type of analysis can be described as qualitative description. My approach could also be considered hermeneutic, meaning that I seek to better understand the whole through the details and the details through the whole. I repeated this process several times. Content analysis, a method for interpreting the meanings of texts, is typically considered an integral part of qualitative research. In this study, however, I have tried to avoid overly interpreting the data.

Qualitative description is often considered a rather basic form of research and is not often included in the methodological literature among the more interpretive qualitative methods. However, especially in practical disciplines where researchers are interested in a practical phenomenon, the basic method of qualitative description has proved to be one of the most commonly used methodological approaches. (Sandelowski, 2000)

All research, especially qualitative research, requires interpretation, based on understanding of the facts, context and researcher's own background, and there is probably no such thing as pure interpretation. However, the ”low-inference” of qualitative description, or in other words, staying close to the data, also helps others interested in the research topic to understand the research object in a coherent way. Qualitative description is low-inference in the sense that it tries to describe facts as they are, in “everyday language”, while avoiding unnecessarily describing things through a very philosophical or conceptual, abstract framework. As a summary and general rule of qualitative description is to avoid multi-layered interpretation, the so-called interpretation of interpretation. (Sandelowski, 2000)

One of the hidden background purposes of this study is to help the case organization better understand the construction of its own information security practices, and therefore in this study I aim for a description of the organization and events that is not too far from the data in terms of interpretation. Since the focus of the study is on information security practices as a temporal and local phenomenon, I believe that the readers of this study will appreciate a so-called straight description of the phenomenon itself – who, what and where –, and in this case a qualitative description is the methodologically correct choice (Sandelowski, 2000).

4 Case Organization and its Context

The organization under study is a Finnish subsidiary of a European company operating in 15 countries and providing business process outsourcing services. It serves a wide range of clients but mainly focus on large corporate clients. Due to the confidentiality of the organization, it will be referred to as case organization in this thesis.

The organization selected as the context for the study provided me with a comprehensive and somewhat unusual opportunity to examine the factors that have influenced the formation of situated information security practices. In literature, organizational information security has usually been examined in the context of a standalone and independent entity. This study helped me better understand the position and pressures of a dependent subsidiary, which may not necessarily be able to make all decisions itself, for example due to directions from the parent company.

The study was also well-timed. As a result of a recent corporate acquisition, the organization's ownership has changed, resulting in the need to adjust their information security practices. The transaction was carried out by transferring ownership between two operating companies, meaning the buyer was a strategic buyer, as opposed to a financial buyer (Martos-Vila et al. 2019). Such a transaction has many consequences. For example, the strategic buyer may require the acquired company to adopt its information systems and security practices. For these kinds of reasons, post-merger integration takes place after the transaction closing date. Due to the post-merger integration, the technology landscape of the organization is changing, and it is temporarily dependent on the IT and security services of both the old and new owners.

4.1 Corporate Acquisition as Context

Corporate restructuring is a part or a consequence of the company's strategy to reorganize its operations or financial structure in a way that is more beneficial to the company (DePamphilis, 2016). These reorganizations can take the form of internal, so-called organic transformational actions, but the literature suggest that operational restructuring refers specifically to the *divestiture of a business*, and the *acquisition of a business* (DePamphilis, 2016). In the case of divestment, or the sell-side, the objective of the transaction may be to reduce costs by shedding unprofitable businesses, or to redirect resources to other businesses. On the other hand, in case of acquisition,

or the buy-side, the objective may be, for example, to achieve economies of scale, to acquire new capacities or capabilities, or to expand into new markets (DePamphilis, 2016). The term *Mergers & Acquisitions* (*M&A*) has come to be used to describe the buy-side transaction-related activities. The term is widely used, but not strictly defined, in the sense that there are examples in the literature where M&A can also include sell-side activities (Schade, 2013).

In general, a corporate transaction consists of the parties signing an agreement (the *signing*) and transferring the purchase price in exchange for ownership (the *closing*) (Subramanian & Petrucci, 2021). But there are often legal, financial or operational reasons why the two do not occur in immediate sequence (Subramanian & Petrucci, 2021), and typically the technical aspects of the transaction include, in addition to signing and closing, the period between, during which the terms of the transaction is fulfilled. In practice, during this period, the target sold is divested from its parent company, meaning that the seller performs the separation. The target may be spun off into a stand-alone company, or the buyer may, after closing, integrate the target into itself to some extent. Once the purchase price has been transferred in exchange for ownership, an acquisition has occurred. What happened before the closing of this trade can be called the pre-acquisition phase, and after the closing is the post-acquisition phase.

Sometimes the complexity of the separation or the integration of target is high, for example when the target is entirely dependent on the IT or other services of the seller. In such cases, a *transition service agreement* (TSA) may need to be concluded, which guarantees the provision of needed services from the old owner to the target or the new owner for a certain period of time after closing. The TSA ensures a transition without compromising the target's business, allowing the target to continue using the seller's systems until they can be replaced over time by the buyer's systems.

The case organization has been acquired by another company, resulting in a change of ownership. In this transaction, the buyer, the current parent company of the case organization, expanded its operations into the Finnish market by acquiring an existing Finnish company. In the literature, such a transaction is called a *horizontal acquisition* because the target of the acquisition is related to an existing business of the buyer, and the buyer and the target offer the same services but in different markets (Ibrahimi, 2018). Strategy and M&A practitioners usually refer to this as *market ex-*

pansion, or more specifically, *geographic expansion* or *expanding the geographic footprint*. Another reason for this acquisition was so-called *capability uplift*, meaning that the buyer gained expertise that it did not previously have.

The buyer, the current parent company, planned an absorption, meaning that the acquired case company would fully merge with the new parent company in terms of operating model, meaning policies, processes and systems. Both IT systems and information security as a whole are affected by this. The study was conducted during a transition period. Post-merger integration was underway. The buyer's systems were being implemented, and the seller's systems were being phased out. Information security practices were updated to align with the buyer's policies and requirements.

4.2 Complex Ownership Structure

As a result of the acquisition, the ownership structure of the organization naturally changed. When the buyer is a strategic buyer, it is quite common for new owner to be a multinational organization with a complex corporate structure. This is also the case here. The buy-side ultimate parent company is a multinational *conglomerate*, and one of its divisions operates in the same industry as the case organization and holds numerous commercial brands in its portfolio. Several layers of ownership divided into different legal entities exist between the case organization and its new ultimate parent.

The new owner is a *company group* organized into a chain structure. A company group means that the structure includes several nominally separate companies, for example in terms of commercial brands, but these companies are under the financial control and direct or indirect operative control of a single management. Legally, these are different companies, but from a financial perspective, they ultimately generate value for the same ultimate parent and the same beneficiaries. (Dong et al., 2025)

The ownership structure has an impact on the internal policies that are imposed on case organization by its parent companies. The external industry regulation of parent companies also imposes some requirements on case organization. For example, because the ultimate parent company operates in several industries, the regulation of those industries is reflected in case organization's

parent's parent's internal policies, which case organization must therefore follow, even though the legislation of those industries does not bind case organization directly.

This complex organizational structure has an impact on how information security is built in the case organization. Von Solms et al. (2011) pointed out that "a properly implemented Information Security Governance framework" should enable direction from the strategic level to the tactical and, ultimately, the operational level. It should also enable as control, meaning reporting, from the operational level to the tactical and, ultimately, the strategic level. From the perspective of information systems and information security, the strategic level referred to by von Solms et al. is at the parent's parent level in the case organization's current operational architecture. In other words, the organization is dependent on its parent's parent for information system services and information security. This dependency is also reflected in the policy architecture. In an earlier article (2006), von Solms and von Solms discussed this direct-control cycle in more detail, noting that it is one of the core principles of corporate governance. Regarding the case organization's information security practices, this principle is implemented as a chain structure. The strategic level, meaning the target and policy setting level, is at the parent's parent level. The tactical and operational levels are divided between the case organization and its parent company.

4.3 Interdependence in the Areas of Information Technology and Security

The case organization has its own operational ERP system, originally hosted in a local data center. Following a series of acquisitions and mergers, the organization became part of the company now known as the previous owner. The ERP system was transferred to that company's data center, which were acquired through outsourcing and are located abroad. Since then, the case organization has been responsible for application maintenance, meaning that the super users and process developers are from the case organization. The old parent company has since been responsible for the infrastructure and outsources the maintenance work to third parties. This ERP system is still in use.

Over time, a set of typical business applications has emerged around this ERP system. These applications are integrated with each other, allowing data to flow from one system to another. Some of these applications are cloud-based applications operating in SaaS model. This means that the or-

ganization is not responsible for maintaining them but is responsible for example system integrations. The case organization also has public-facing applications developed for customer use. Third parties developed and maintain these applications. In terms of basic IT infrastructure, the company is dependent on its former parent company. In practice, the case organization is only responsible for network connections at its offices and for end-user devices.

Since ownership of the case organization has already been transferred to the new owner, but their business applications are not yet in use, a Transition Service Agreement has been agreed upon for the duration of the post-merger integration project. In this agreement, the former owner provides the case company with a secure IT environment and enables secure connections to the new owners IT infrastructure, and collaboration and communication channels. The case organization, however is obliged to comply with new owner's IT usage and information security policies. At the same time, of course, because the old owner's systems are being used, the case organization follows its policies and guidelines.

5 Situated Information Security Practices

This section aims to address the question: “What information security practices have been localized, and where did the ideas for them originate?” First, I will discuss the themes that emerged from data. Then I will discuss the information security practices belonging to these themes, one by one. To protect the anonymity of the case organization, I will discuss them at a high level and refrain from going into technical details. Similarly, I will refrain from criticizing current practices because the main objective of this study is to map out how these practices emerged rather than discuss their suitability in depth.

5.1 Thematic Categorization of Current Information Security Practices

I analyzed the case organization’s current information security practices. This analysis was base primarily on the organization’s documents, particularly policy documents. In addition to these documents, I reviewed other information security documentation to supplement my understanding. Furhermore, follow-up interviews supplemented and refined my understanding of current information security practices.

Before conducting the actual data-based analysis, I outlined preliminary themes based on my understanding of the current information security practices. As analysis progressed, new themes emerged from the data. The analysis followed hermeneutic logic, or in other words, circular process of refining understanding. During the initial interview, I addressed the big picture. The understanding gained from this interview was supplemented as details emerged from the documents. I repeated this process several times, and as a final step, conducted three follow-up interviews. The final, refined themes are described in table 2.

Some themes were visible directly in title of document, some emerged by analyzing the content of the documents, but many sub-themes were not addressed in the documentation. Some of these sub-themes were identified during the first semi-structured interview. However, participatory observations was particularly valuable when defining these themes. Since I participated in the daily life of the case organization as part of the team, I was present when more specific information security issues were discussed. These discussions led many times to the deeper technical discussions with responsible individuals.

Table 2. Analytical Themes on Current Information Security Practices

Category	Theme	Sub-themes
Governance	Information Security Governance	Management commitment to information security, roles and responsibilities, information security policies, compliance, and testing information security
	3rd Party Management	3rd party contracts, monitoring, internal and external reporting, Application security
Narrowing the Scope of Attention	Asset Inventory	The ownership, number, identification, classification, prioritization and the life cycle management of assets
	Basic Security Hygiene	Identity and access management, endpoint protection, data network protection, protection of business solutions
	Vulnerability and Batch Management	Vulnerability identification, batch management, configuration management
Risk Assessment	Critical Processes and Systems	Systems and processes that are key to managing operational risks
	Critical Data	Data that requires protection due to operational risk, or regulatory or compliance requirements
	Information Security Risk Assessment	Basis for risk management, such as risk classification and limits; risk management implementation and procedures, and risk treatment
Incident Management	Incident Detection	Logging and incident monitoring, internal incident reporting
	Incident Response	Roles and responsibilities, procedures
	Business Continuity Management	Business impact analysis, business continuity and disaster recovery procedures, training of these procedures, backups
Awareness & Training	Information Security Awareness and Training	New employee onboarding, policy and procedure communications, threat environment, targeted user training and simulations

5.2 Information Security Governance

The first analytical theme I will discuss had already emerged from my preliminary expectations. I expected that an organization like the case organization must have some kind of information security governance. It is worth noting that based on the data, that the information security direct-control cycle discussed by von Solms and von Solms (2006) and von Solms et al. (2011) exists and is clearly observable. However, as I mentioned earlier in Chapter 4, this direct-control cycle is divided between several parent subsidiary pairs. In practice, this division of the direct-control cycle into several organizational levels primarily falls under the theme of information security governance, but it also extends to all other themes. The position of subsidiaries and the complex ownership structure are reflected in all aspects of information security.

Figure 2 illustrates the direction of the direct-control cycle within the policy architecture of a case organization. Policies and procedures marked as "local" are those of the case organization or its parent company. We can consider these to be on the operational or tactical level. In this figure, I have, for illustrative purposes, labeled the legal entities at different levels with letters of the alphabet. The case organization is A, and its parent company is B. Level C could be considered strategic because C is an independent entity with its own systems and policies. The case organization either uses or is transitioning to use C's systems. Above C are D and E, with E being the ultimate parent company. Company C is therefore the independent and decision-making organization described in academi information security literature, while Company A is a subsidiary that is completely dependent on systems provided by others and must comply with practices and guidelines set by others.

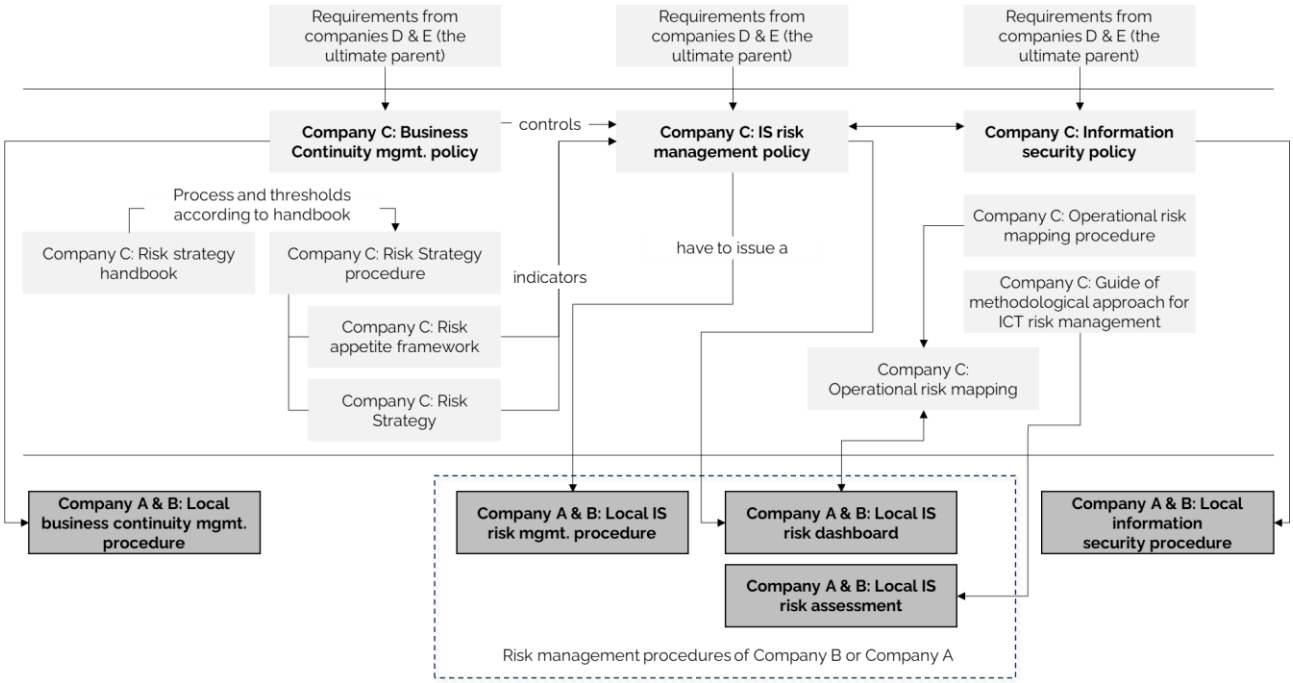

Figure 2. Example of Policy Architecture

This same complex ownership structure is reflected in roles and responsibilities, one of the key areas of information security governance theme. The Chief Information Security Officer or CISO, works where information security is governed, meaning the parent's parent of the case organization, represented by the C in the figure. As part of the parent company, or company B in the figure, there is a Regional Information Security Officer who is responsible for implementing policies and monitoring compliance with these policies at the parent company level. In practice, this

means working together with the case organization and its sister companies. The case organization employs two Information Security Administrators. They are responsible for implementing, monitoring and developing local information security practices. They report directly to the Regional Information Security Officer. However, because information security plays a significant role in local operational risk management, which is led by the CEO, they also collaborate closely with the local risk management team located in the case organization.

The ownership structure also clearly impacts third-party management, which I have classified as part of the security governance. In practice, the former owner remains responsible for most of the information technology used by the case organization. These systems will be replaced by similar systems from the new owner once the post-merger integration is completed. However, the case organization has public-facing services developed by third parties. Although the case organization owns these services and is ultimately responsible for these, maintenance and security are the responsibility of the third parties according to the terms of the agreements. The case organization has processes in place to handle matters related to the agreement, and that is also required by the new parent company via separate policy. Other third parties also test these services when significant changes are made.

The role of the subsidiary surprisingly affects the case organization. Because case organization provides business process outsourcing services to other companies in a highly networked industry, it is occasionally required to provide formal evidence that it is a reliable business partner in terms of information security. Since this is a subsidiary dependent on two owners, old and new, gathering and providing such evidence is not always easy. Since neither the old nor the new owner is certified under any widely recognized information security standard, demonstrating this kind of qualification requires more effort and justification than it does for certified organizations.

5.3 Narrowing the Scope of Attention

In his text, Kamran (2013) presents an interesting analogy to information security risk management: A chess player focuses their thinking only on a specific, limited area of the chessboard because that is where the events that determine the outcome take place. Building on this analogy, I add that the player must also be aware of occurrences outside of this limited area. The player

must know the positions and statuses of the pieces outside the limited area so that nothing diverts attention away from the central event or becomes a new central event.

I remember reading about this analogy before, but I thought of it again when categorizing the data of this study. This kind of baseline awareness of status and maintenance of basic hygiene didn't really belong in the category I call information security governance. I also wanted to highlight the difference between this and actual risk assessment. As study progressed, I concluded that, to enable appropriate risk management, risk assessment should focus on a limited area of the chessboard while treating the surrounding area as more routine yet still important. The biggest difference lies in the practices, for example, how activities within an organization should be organized. Risk assessment is inevitably more project-based and requires focus and resources, whereas maintaining this kind of basic hygiene should be more process-oriented and require less attention or resources in the everyday life of organizations. Therefore, a new distinguishing category was needed. This category is named as such because these activities should only require a small amount of energy in daily life of information security professionals, so that more demanding tasks can be focused on when necessary.

This category consist of three key factors. First, identifying what the organization has that could pose a security threat, either currently or in the future. Second, you need to identify the vulnerabilities of the assets and address them. Third, ensure that the assets are correctly configured, meaning that they perform only their intended functions. And these measures should be organized so that the activities are continuous and regular.

First, it is necessary to understand what within the organization could pose a threat to information security now or in the future. The purpose of this is to map the attack surface. Only what is known can be protected – protection being a conscious activity. When it comes to assets that could pose a security threat, physical devices, particularly end-user computers and mobile devices, intuitively come to people's minds. However, organizations have other physical devices that should not be visible to end users, such as network devices and servers. Servers are the prime example of devices that usually are either forgotten to be upgraded and patched or, in the worst case, forgotten to exist altogether. According to the literature, applications are also something that should be in-

ventoried. Based on my professional experience, I can say that it is surprisingly common for organizations to have so many software programs that not even someone in the IT department knows them all.

In many cases, a subsidiary is a local affiliate, meaning a legal entity established to officially represent the parent company in a specific country. In these cases, for practical reasons, it is often decided that the subsidiary should purchase or lease basic IT equipment from local suppliers. The organization is then responsible for maintenance and lifecycle of these devices. The parent company often provides disk images that can be set up locally on these devices, enabling them to operate within the parent's network environment.

Because human labor is expensive, organizations strive for cost-effective personnel structure, and generally organizations do not have excess employees. The limited resources an organization has to carry out its tasks should remain close to its core business. Non-core business tasks should be outsourced. In my experience, modern IT management works exactly like this. Business and support function applications are generally delivered as services, meaning they are standardized applications whose maintenance and development are handled by an external organization. Only applications for which there are no market solutions that meet business-based requirements should be maintained in-house.

The operating model descriptions in the previous two paragraphs illustrate roughly how the case organization operates. Asset registers were originally created for financial reasons, but once it was realized that they are also basic requirement for information security, they became strongly required. In case organization, the origin of the practice can be tracked back to the parent companies. Current parent company determines an acceptable method for maintaining asset inventory using their own policies. The current parent company requires the case organization to regularly provide evidence that its asset inventory is up to date. The old parent company utilized the procedure.

In situations described above, even though inventorying assets is straightforward, mapping the attack surface is complex. Then the asset inventory itself is an inventory of physical devices and ap-

plications. If an organization has been using an internal network infrastructure, outsourced applications can lead to a complete change in the attack surface topology. In this case, some degree of the zero-trust architecture should be implemented. The case organization has been using these outsourced applications for quite some time, and MFA infrastructure, for example, has been provided to it through its parent companies.

Once the assets to be protected have been identified, it is important to ensure that there are no obvious vulnerabilities in these. Regarding end-user devices, the case organization itself monitors significant vulnerabilities. Otherwise, automated software updates does the patching of vulnerabilities in end-user devices. Third parties are directly responsible for updating application and their related infrastructure. However, the case organization approves updates for some services, mostly the public-facing local applications. The organization also uses a third-party service that provides them with a regular list of vulnerabilities detected in their assets.

Basic IT infrastructure services, such as, identity and access management and data network connections and virtual private networks, for example, are provided by the previous owner. The previous and current owners have agreed to a Transition Service Agreement, which means the former owner is responsible for providing these services until the post-merger integration is finished. In practice, the previous owner still controls the entire IT infrastructure services, and the case organization don’t have any control over these.

The case organization utilizes effective practices for asset inventory, vulnerability identification and patching, and basic security hygiene. This allows the organization to focus more energy on the more challenging information security tasks. It is important to recognize that these practices were created externally, and the case organization is not an active participant in their development. Rather, it has adapted to circumstances that have developed and continue to evolve over time.

In theory, it is difficult to identify any concrete institutional pressure in this regard because institutional pressures primarily affect the parent company. Instead, the data revealed findings that are consistent with idea of organizational contingency, such as the developments in organization structures, or in complex ownership structures in this case, affects heavily to the information security practices.

5.4 Risk Assessment

Risk management is the foundation for developing information security and maintaining a secure state. As previously stated, according to von Solms and von Solms (2004), the most important question for those responsible for information security in an organization is, “Against which risks must the information resources be protected?”. However, we should first take a step back from this question. There are at least two approaches to answering this question, neither of which is sufficient on its own. The first approach is based on the impact on business operations, while the second is based on asset vulnerabilities. Both approaches evaluate threats and their potential impact on the organization, but their underlying methodologies differ slightly. The business impact approach examines systems and their potential impact on the organization in the event of an incident. In order to perform a business impact analysis with the required accuracy, it is necessary to understand critical business processes. The asset-based approach begins by identifying assets and assessing the risks associated with each one. To ensure a comprehensive risk assessment, both approaches must be used. The parent company of the case organization requires a business impact analysis first. Only systems that exceed a certain threshold undergo a more in-depth asset-based risk assessment. Technical and architectural factors, such as how easily an attacker can move laterally, affect the risk posed to the organization by an individual vulnerable asset. These factors also affect whether the model presented by the parent company of the case organization is considered sufficient. In this case, given the circumstances and local complementary practices, the model is sufficient.

From an information security perspective, the organization's risk management is structured so that two reporting lines work together. The first is the business and its risk management function. The local risk management function reports to the Chief Executive Officer and to the risk management function of the parent company. The risk management function is responsible for operational risks, while the information security function is responsible for information security risks that are part of operational risks. Other risks may include financial risks, which are usually the responsibility of the organization's finance department. Decisions on risk treatment and risk appetite are made by the parent company in accordance with directed procedures and value limits.

As the head of the case organization, the Chief Executive Officer is responsible for its results and, therefore, for risk management as well. Although direct operational risks, such as downtime of

business-critical systems, were identified as the most significant, reputation risks are becoming an increasingly important factor in risk management. The organization operates in a highly networked industry where trust is fundamental to doing business. Business partners, such as customers, expect a secure IT environment and protection of their data using appropriate measures. Case organization has comprehensive processes for managing, protecting, storing, archiving, and disposing of data.

The information security function reports to the IT director locally and to the Regional Information Security Officer at the parent company. Currently, the local information security function is only minimally involved in risk assessment. Due to the corporate acquisition, most of the currently used applications are systems belonging to the previous owner. These systems are used not only by the case organization, but also by the former owner's own end users. The former owner is fully responsible for the security of these systems. However, since the new owner's systems have not yet been implemented, the case organization's information security function is only responsible for risk management for a new locally owned, public-facing applications.

As part of post-merger integration process, the new owner has also initiated takeover measures regarding information technology and security. Takeover means that the new owner will take control over the company it has acquired. Typically takeover plan is divided into different phases. The first phase is called Day 1 plan. During the first day of ownership, typically bank accounts and treasury are taken over, the necessary reporting lines are changed and any brand related changes are made. Later, various functions are taken over until, towards the end of the post-merger integration period, the business processes and related systems are taken over or migrated to existing parent company's systems. Since the case organization is a local affiliate and parent's only legal entity in the country, some of the typical measures mentioned above do not apply to it. Takeover measures related to IT systems and security have already begun. The order of these activities is also very logical. First, a set of standards and policies is established to set the minimum requirements for secure system usage and sustain behavior. Next, the acquired company is given access to basic IT services and infrastructure, such as identity and access management. Lastly, the systems will be integrated. The business applications are typically the most difficult to integrate because business processes and applications are typically closely coupled.

The new parent company has a comprehensive set of risk management policies, procedures and guidelines, some of which concerns information systems and information security. See Figure 2. Subsidiaries must comply with these, and additionally they need to establish local practices. Subsidiaries must implement a documented procedures to guide the local practices in information systems, information security, and business continuity.

Same observation applies to risk assessment as to the previous category, the institutional pressures primarily concern the parent company. However, participatory observation shows that new customers impose coercive pressure in terms of risk management. These potential future customers are interested not only in whether the case organization is reliable partners that appropriately handles information security with a risk-based approach.

5.5 Incident Management

The incident management category covers actions taken by an organization in the event of a security breach. In this context, an incident can mean more than just a security breach, as the same or similar procedures are also followed in cases where a system is out of service, even if it is not a security breach.

Incident detection is an organization's ability to identify unusual events. Typically, companies monitor system logs from key software components, such as firewalls, operating systems, server software, and application software, using a single log monitoring system. This type of system is called a Security Information and Event Management or SIEM system. There are also systems designed specifically for automatic incident detection. These systems are known as Intrusion Detection Systems or IDS. Technically this kind of logging system can be implemented in various ways. For instance, log data can be collected in a single database, or one logging system can be given access to the log data of other software. The collected data may include for example data of user logins and configuration changes. Depending on the technologies used, anomalies can be identified manually or automatically.

Incident detection remained a blind area in the data, in the sense that only the semi-structured interview revealed the product used by former parent company to collect these logs. And documentation reveals the local incident management procedure. I interpret this to mean that the case

organization does not have truly accurate information on how incident detection is handled. However, data reveals enough about the local process: the former parent company reports findings to the case organization when necessary. This triggers a local incident management procedure, which includes roles and responsibilities, procedures for decision-making and further actions. What also raised from the data on this local procedure is that such situations are very rare and organization has not been practicing these kind of situations. The procedure itself is straightforward. This can be problematic in situations where a system has actually been compromised because such situations can be quite complex.

Although the security incidents have not been practiced within the case organization, based on data the staff seems prepared. This is due to their regular training in traditional IT business continuity. Business continuity refers to how an IT department, or the whole organization, recovers from the incidents to resume normal operations, for example, by using backup copies. The case organization has strong policies and procedures in place for such situations, and they are practices regularly. This was clearly part of the previous owner's culture, but no data has yet been recorded on the new owner's practices. The case organization operates in an industry where information systems do not necessarily have an immediate impact on operational activities. Therefore, the organization should be able to tolerate system outages that can be resolved in a timely manner according to business continuity management procedures.

The data provides a varied view of this category. On the one hand, the subsidiary status is evident, as the case organization has little contact with or influence over information security incident detection and response processes. But on the other hand, there's a clear focus on more traditional IT business continuity management. This can be explained by the dynamics of responsibility resulting from organizational structure, or ownership structure, and technological interdependencies. In terms of information security, responsibility is divided between the current and former parent companies in a Transition Service Agreement. However, the case organization is an independent legal entity, and most factors affecting its financial results fall under local decision-making authority. The same is reflected also in risk assessment category. Risks that impact the operating result, such as systems being out of use for long periods, are the focus of risk management function. Information technology risks can be easily incorporated into these risks, and the cost of lost business activity due to downtime can be easily calculated. However, information security risks for which

no price can yet be determined, such as data breaches or ransomware attacks, may be more difficult to incorporate into operational risk management. This dynamic is made even more interesting by the fact that the reporting lines are split into two. First, the local information security function works with local operational risk management. On the other hand, the parent company's information security function manages risks from a different perspective. As I understand it, this phenomenon is not uncommon in any company, whether it is a subsidiary or not. Rather, it is a completely normal situation.

5.6 Information Security Awareness and Training

Information Security Awareness and Training differ from other categories in that the case organization has strong control over these practices. The case organization has been able to supplement the service provided by the parent company with training courses offered in local language and phishing simulations well-suited to local conditions, even though the parent company's policies govern this area.

"Users have long been regarded as the weak link in information security" (Schultz et al., 2001). Although it is difficult to provide any definitive arguments for this statement, it seems plausible that, in an environment where the Narrowing the Scope of Attention category is in order, malware will certainly find its way in through email than through a firewall. The purpose of these practices is to ensure that the organization's investment in information security is not made useless by personnel allowing attackers to gain access through clicking on links.

The case organization uses a mini-course service provided by a local third party. Mini-course means that end users occasionally receive email invitations to a course page covering a specific information security topic that all employees need to know. The course is tailored to the organization. It is conducted in the local language, and the topics and examples used in the training are relevant to the local context. In my understanding, all topics intended for study are covered during the year. Therefore, this fulfills the definition of annual information security training.

The case organization uses a phishing simulation, which involves sending harmless phishing emails to users. Like real phishing emails, these messages contain a request to click on a link. Users can identify these messages as phishing attempts based on the same characteristics that make real

phishing messages recognizable. Users must identify and report these messages in accordance with the appropriate procedure. This servers to educate users, but also to monitor their behavior. If necessary, information of user behavior can be used as one of the criteria for risk assessment.

Examining this category from the perspective of institutionalization makes it clear that institutional pressures, whether mimetic, normative, or both – have impacted the adoption of such practices. The data does not provide further details on how these arrangements were reached. In my eyes, all peer companies have similar practices in place, so, in addition to normative pressures, mimetic pressures are likely at influence as well.

6 Discussion

The research question for this study was, *"How have the internal, situated, information security practices constructed in a subsidiary company?*". Three sub-questions were used to answer it. I will discuss each sub-question and its results individually below. First, however, I will discuss the study's more detailed course.

6.1 Research Process

The study is based on the understanding that organizations' decisions regarding information security practices are not always based purely on risk management and economic considerations. Clearly, factors such as regulation, internation information security standards, the ease with which professionals can network have an impact. Information security's role in building trust, both internally and internationally, also influences companies' choices regarding information security practices.

I encountered a contradiction: although we live in the midst of multinational companies, the academic and professional information systems or security literature still doesn't recognize the role of subsidiaries as much as it should, given their current practical importance. This problem may not have existed before because properly implemented information security practices were not a prerequisite for cooperation. Nowadays no on will work with you if your information security is not properly arranged. In theory, this should not be a problem for subsidiaries either. However, as the study showed, subsidiaries are not in the same position as independent companies when it comes to information security. This has many implications for practice.

To answer the research question, I conducted a three-month case study of a company in an interesting situation. This company is a subsidiary that was recently the target of a corporate acquisition. This provided me with valuable insight into the information security practices of subsidiaries.

The main source of data for this study is the case organization's information security documentation. I also conducted one group interview and three individual interviews. I supplemented the source data with my observations while participating in the case organization's daily activities. I

helped with practical tasks, joined the lunch crew, and spent time getting a feel for everyday life at the organization. I attended the case organization's weekly sports club every Friday.

Since the source data was qualitative, I needed to make a simple thematic classification based on my preliminary assumptions and refined it as the research progressed. The end result was the fifth chapter of this study, in which I described my understanding of the case organization's information security practices, as well as the factors that influenced their development.

6.2 Outcomes of Research

Before conducting the study, it was important to understand the context of the organization. By context, I mean answering questions such as: What does the organization sell? Who are its customers? What is its internal organization structure? What kind of group structure does the parent company have? What does it mean to be the target of a corporate acquisition in practice? What kind of technology landscape do they have? What kind of business processes do they have? And many other questions.

I was surprised by two things when I examined the context of the case organization. First, I was surprised by the size of the entire group. There are four layers of operational companies between the case organization and its ultimate parent company. Second, I was surprised by how much the corporate acquisition and following post-merger integration complicate the daily life within the case organization, especially within its IT function.

The first sub-question of the study was: "*What are the localized information security practices?*". The purpose of this question was to understand the local information security practices in place within the case organization. Together with Chapter 4, it was intended to provide a foundation for further exploration of how these arrangements have been formed or how they have evolved over time.

The first sub-question was also associated with the first research result. The case organization had implemented nearly all of the information security measures that I would expect from a company of this type. However, almost none of these measures were developed specifically for this organization. Rather, the organization used them as if they were borrowed or rented. This is natural, of

course, given the context. The organization was originally a subsidiary of a larger company. Then, it was acquired by an even larger company and became its subsidiary. At some point, I though of the analogy of a tenant and how a tenant must adapt. Yes, they know how to adapt. That organization is extremely skilled what they do. Despite having limited resources, the IT function which includes information security, does an impressive job.

Another research result relates to organizational structure and policy architecture. Initially, I assumed that the case organization is a subsidiary of a group consisting of its parent company and sister companies. I also assumed that the group's head office provided group functions, such as finance, human resources, and information technology, to the subsidiaries. However, I was surprised to realize that the group was actually the parent company of the parent company. This meant that what I thought was a two-tier organizational structure was actually a three-tier structure. When considering an information security management system, one wouldn't immediately think that it should be implemented in such a structure. And of course, if the group crosses borders, it is perfectly logical that finance and human resources functions must be local due to legislation and liability issues.

The second sub-question of the study was: "*What material factors have affected localization?".* The main purpose of this question was to find out if contingency theory could explain the emergence of information security practices. This question aimed to identify the material factors, such as organizational structure or technology, that influence the development of information security practices in subsidiaries. These issues have been studied very poorly form the perspective of subsidiaries, so highlighting them could be valuable for academic and practical discussions.

The research data revealed that the organizational structure is the most significant material factor influencing the development of situated information security practices in this subsidiary. In practice, this three-tier structure strongly influences roles and responsibilities, affecting all the categories presented in Table 2.

Another significant factor was the corporate acquisition that took place. Following the acquisition, post-merger integration naturally led to technological dependence on the previous owner. However, I consider this to be a temporary situation. Furthermore, I lack sufficient data to generalize

about the impact of acquisitions on information security arrangements. The IT and information security arrangements of corporate acquisitions have been studied more extensively than those of subsidiaries.

In reflecting on contingency theory, and based on this study I can generally conclude that an organization's configuration has a significant impact on the development of information security practices. Therefore, it is reasonable to conclude that it also affects information security.

The third sub-question of the study was: "*What non-material or social factors have affected to the localization?".* The main purpose of this question was to find out if institutional theory could explain how the information security practices emerge. The value of this question was lower than expected. Since the case organization is responsible for only two aspects of information security, namely end-user IT and training, the institutional impacts mainly affect organizational levels other than the case organization.

Institutional pressures are most clearly visible in the information security awareness and training category. The case organization has acquired training services from 3rd parties, including mini-courses on information security for end user training, as well as phishing simulations for end user training. End users are also assisted by notifying them of the last security updates, for example on mobile phones, as soon as these become available. While the specific background influences on these practices cannot be determined from the data, it is reasonable to assume that they are ultimately the result of many different institutional pressures.

The most significant finding related to this question is that new customers exercise coercive pressure on case organization. This is largely due to the industry: case organization operates in a business-to-business context, customers expect the companies with which they enter into business relationships to manage information security responsibly. While observing the organization's daily operations I witnessed a situation in which completing and information request list was a prerequisite for establishing a business relationship. This list contained a subset of ISO/IEC 27001 controls and the case organization was asked to respond regarding its practices in this regard.

6.3 Research Critique

Since this study is also a thesis, my goal was to learn how to apply at least one qualitative research method well. I learned a lot, of course, but during the course of my research. The first lesson I learned was that research questions are very important, because everything happens according to the terms set by the questions after they have been formulated. I have read that qualitative research is flexible, and it's normal for the topic to become more specific over time. However, once the research questions are set, the research strategy is chosen, the data collection begins, and the research moves forward. While the research questions did become more specific during the study, some of the initial data is less representative than it was in the original research design.

Although qualitative description is a good basic method, and the chosen research topic does not require much interpretation, these methodological choices undoubtedly left the study superficial. If I were to conduct the study again, I would choose a more interpretive approach and collect more data through interviews. And, if I were to conduct the study again, I would adhere more strictly to the traceability requirement. This would also force me to prepare thoroughly for the various research stages and tasks.

As a researcher, I recognize that I tend to rush to conclusions based on heuristics. This tendency may be evident in the text, and the treatment of certain issues and conclusions may seem overly simplistic as a result. I have put in a lot of effort to manage this issue and have attempted to eliminate it to the greatest extent possible during my research.

The context of the case organization special. In fact, one might consider it too special. This case study almost had to be just exploratory because the organization's almost unique characteristics, such as its complex ownership structure, interdependence with both, former and new owner, make generalizations difficult. Nevertheless, I hope that this study fulfills the requirement of producing new information. And because the situation of the case organization is so special, my theoretical framework appears somewhat naive. In this case, institutional pressures are overshadowed by prevailing situation.

6.4 Contribution of This study

This study is an exploratory, naturalistic research project investigating how subsidiaries construct information security practices. This is a new research area with no prior studies. This study's main contribution is presenting the research area as a new interesting problem field. At the same time, the study produced new information about what these situated information security practices may entail. Additionally, this study highlights initial observations and influencing factors. Organizational structure strongly influences the formation of information security practices. Institutional pressures also affect subsidiaries, but to a much lesser extent than independent companies.

6.5 Research Ethics Considerations

An appropriate research permit has been obtained for this study, signed by representatives of both the case organization and the educational institution.

Because of the sensitive nature of the research topic, I have taken care to protect the organization's anonymity in this study report. And, because topic is sensitive, this research was conducted using a computer and data repository provided by the case organization. All data related to the study is held by the case organization in a secure data repository. An appropriate data management plan has been created for this study. Tables and images containing policy names or other potentially sensitive information have been reviewed by a representative of the case organization.

I have taken advantage of the free online service DeepL Translator published by DeepL SE by using its DeepL Write feature, which suggests how to better write a sentence that is already in English. This has helped me, for example, to use American English consistently.

6.6 Entry Points for Further Research

My study on information security in subsidiaries was just beginning. There are many interesting topics to explore. However, I strongly recommend that future researchers choose a more conventional case to gain an authentic understanding of the mechanisms affecting the information security of subsidiaries.

The impact of a two- or three-tier organizational structure on information security practices is an interesting topic. What impact does this structure have on information security posture, maturity or, for example, the number of incidents.

During my research, I came to believe that contractual obligations alone are insufficient in cases of information systems outsourcing. More comprehensive risk management is needed. Which factors should be considered when drafting an outsourcing agreement, and how should the risks associated with outsourced services be managed throughout the service lifecycle?

7 Conclusion

This study is the first to examine the information security practices of subsidiaries, how they are formed, and the factors that influence their formation. The most significant finding is that the organizational structure has a strong impact on the formation of information security practices. This is because a subsidiary is always subordinate to another company, resulting in the division of information security practices between these two, or sometimes three, levels.

Another significant finding is that institutional pressures do not impact subsidiaries in the same way that they impact independent companies. Subsidiaries have less decision-making power to adopt information security practices as a result of these pressures. However, the study revealed a potential indirect effect: if the parent company is affected by these pressures, such practices spread through it.

This research setting forced us to examine the subsidiary's position in relation to the parent company. This does not imply that the position of a subsidiary is good or bad. Rather, it is an interesting topic that offers new and exiting opportunities for researchers interested in organizational information security. This topic is also increasingly relevant, as more and more subsidiaries are appearing around us. In fact, measured by market value, more than one in three Finnish companies is foreign-owned, and most of these are likely to be subsidiaries.

References

Andress, J., & Leary, M. (2017). Building a practical information security program. Syngress.

Baskerville, R., & Dhillon, G. (2008) Chapter 2: Information Systems Security Strategy: A Process View. In Straub, D.W., Goodman, S., Baskerville, R., & Books 24x7 Inc. (Eds.), Information Security: Policy, Processes, and Practices. Routledge.

Benbasat, I., Goldstein, D., & Mead, M. (2002). The case research strategy in studies of information systems. In M. D. Myers, D. Avison (Eds.) The case research strategy in studies of information systems (pp. 78-99). SAGE. https://doi.org/10.4135/9781849209687.n5

Benbasat, I., & Zmud, R. W. (2003). The Identity Crisis within the IS Discipline: Defining and Communicating the Discipline's Core Properties. MIS quarterly, 27(2), 183-194. https://doi.org/10.2307/30036527

Bjorck, F. (2004). Institutional theory: A new perspective for research into IS/IT security in organisations. IEEE. https://doi.org/10.1109/HICSS.2004.1265444

Blatter, J. (2008). Case study. In The SAGE encyclopedia of qualitative research methods. SAGE. https://doi.org/10.4135/9781412963909.n39

Bouraffa, T., & Hui, K.-L. (2025). Regulating Information and Network Security: Review and Challenges. ACM Computing Surveys, 57(5), art. no. 126. https://doi.org/10.1145/3711124

Brown, J. S., & Duguid, P. (1991). Organizational Learning and Communities-of-Practice: Toward a Unified View of Working, Learning, and Innovation. Organization science (Providence, R.I.), 2(1), 40-57. https://doi.org/10.1287/orsc.2.1.40

Bulgurcu, B., Cavusoglu, H., Benbasat, I. (2010). Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 34(3), pp. 523-548. https://doi.org/10.2307/25750690

Büyüközkan, G., & Güler, M. (2025). Cybersecurity maturity model: Systematic literature review and a proposed model. Technological Forecasting and Social Change, 213, art. no. 123996. https://doi.org/10.1016/j.techfore.2025.123996

Carr, S. C., Hopner, V., Hakim, M. A., Hodgetts, D. J., Chamberlain, K., Nelson, N., Ball, R., Jones, H. (2021). Scaling the Security Staircase. Political psychology, 42(4), 575-595. https://doi.org/10.1111/pops.12715

Cavusoglu, H., Cavusoglu, H., Son, J., & Benbasat, I. (2015). Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. Information & management, 52(4), 385-400. https://doi.org/10.1016/j.im.2014.12.004

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. European journal of information systems, 26(6), 605-641. https://doi.org/10.1057/s41303-017-0059-9

Crowe, S., Cresswell, K., Robertson, A., Huby, G., Avery, A., & Sheikh, A. (2011). The case study approach. BMC medical research methodology, 11(1), 100. https://doi.org/10.1186/1471-2288-11-100

Currie, W. L. (2011). Institutional Theory of Information Technology. In Galliers, R., & Currie, W. (Eds.), The Oxford handbook of management information systems: Critical perspectives and new directions (pp. 137–173). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199580583.001.0001

Czarniawska, B., and Joerges, B. (1996). Travels of Ideas. In Czarniawska, B., & Sevon, G. (Eds.), Translating organizational change (pp. 13-48). De Gruyter, Inc. https://doi.org/10.1515/9783110879735

De Bruin, R., & von Solms, S. H. (2016). Cybersecurity Governance: How can we measure it?. IST-Africa Week Conference. https://doi.org/10.1109/ISTAFRICA.2016.7530578

DePamphilis, D. (2016). Mergers, Acquisitions, and Other Restructuring Activities (Eighth Edition). Academic Press.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Towards socio-organizational perspectives. Information systems journal (Oxford, England), 11(2), 127-153. https://doi.org/10.1046/j.1365-2575.2001.00099.x

Dong, Y., Ni, C., Qiao, F., & Zhang, C. (2025). Business Group Analysts. The European accounting review, 34(1), 427-452. https://doi.org/10.1080/09638180.2023.2238787

European Parliamentary Research Service. (2020). Briefing: Directive on security of network and information systems (NIS Directive) (EPRS Implementation Appraisal PE 654.198). European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/654198/EPRS_BRI(2020)654198_EN.pdf

Flick, U. (2022). Setting the agenda – Roles of Design(ing) in Qualitative Research. In U. Flick (Ed.), The Sage handbook of qualitative research design. SAGE Publications. https://doi.org/10.4135/9781529770278

Goel, S., & Chengalur-Smith, I. N. (2010). Metrics for characterizing the form of security policies. The journal of strategic information systems, 19(4), 281-295. https://doi.org/10.1016/j.jsis.2010.10.002

Hall, S., & Liebenberg, L. (2024). Qualitative Description as an Introductory Method to Qualitative Research for Master's-Level Students and Research Trainees. International journal of qualitative methods, 23. https://doi.org/10.1177/16094069241242264

Hamel, J., Dufour, S., & Fortin, D. (1993). Case study methods. SAGE. https://doi.org/10.4135/9781412983587

Harkins, M. W. (2016). Managing Risk and Information Security: Protect to Enable (2nd ed.). Apress. https://doi.org/10.1007/978-1-4842-1455-8

Hsu, C., Lee, J., & Straub, D. W. (2012). Institutional Influences on Information Systems Security Innovations. Information systems research, 23(3-part-2), 918-939. https://doi.org/10.1287/isre.1110.0393

Ibrahimi, M. (2018). Mergers & Acquisitions: Theory, Strategy, Finance. John Wiley & Sons, Inc.

International Organization for Standardization (n.d.). ISO Online browsing platform. [Database] https://www.iso.org/obp/

Kamran, M. (2013). Security Information and Vulnerability Management. In de Tangil, G. S., e-libro, C., & Suarez de Tangil, G. (Eds.). Advances in Security Information Management: Perceptions and Outcomes. Nova Science Publishers, Inc.

Ketokivi, M., & Choi, T. (2014). Renaissance of case research as a scientific method. Journal of operations management, 32(5), 232-240. https://doi.org/10.1016/j.jom.2014.03.004

Khan, W. N., Lee, J. K., & Liu, S. (2025-01-15). Is Cybersecurity a Social Responsibility? Information systems frontiers. https://doi.org/10.1007/s10796-024-10565-z

Knapp, K. J., & Ferrante, C. J. (2014). Information Security Program Effectiveness in Organizations: The Moderating Role of Task Interdependence. Journal of organizational and end user computing, 26(1), 27-46. https://doi.org/10.4018/joeuc.2014010102

Knapp, K. J., Franklin Morris, R., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. Computers & security, 28(7), 493-508. https://doi.org/10.1016/j.cose.2009.07.001

Kostova, T., & Roth, K. (2002). Adoption of an Organizational Practice by Subsidiaries of Multinational Corporations: Institutional and Relational Effects. Academy of Management journal, 45(1), 215-233. https://doi.org/10.5465/3069293

Levy, Y., & Ellis, T. J. (2006). A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. Informing science, 9, 181-212. https://doi.org/10.28945/479

Luoma, T. (2021) Tytäryhtiötalous ja ulkomaiset yritysostot suomessa: uhka vai mahdollisuus? [Subsidiary economy and foreign acquisitions in Finland: threat or opportunity?] (2021:16). Ministry of Economic Affairs and Employment. http://urn.fi/URN:ISBN:978-952-327-721-2

Malatji, M., Marnewick, A., & von Solms, S. (2020). Validation of a socio-technical management process for optimising cybersecurity practices. Computers & security, 95, 101846-17. https://doi.org/10.1016/j.cose.2020.101846

Martos-Vila, M., Rhodes-Kropf, M., & Harford, J. (2019). Financial versus Strategic Buyers. Journal of Financial and Quantitative Analysis, 54(6), 2635-2661. https://doi.org/10.1017/S0022109019000139

Mitchell, J. (2009). Case and situation analysis. In R. Gomm, M. Hammersley, P. Foster (Eds.) Case and situation analysis (pp. 165-186). SAGE. https://doi.org/10.4135/9780857024367.d12

Myers, M. D., & Avison, D. E. (2002). Qualitative research in information systems: A reader. SAGE.

National Institute of Standards and Technology (n.d.). NIST Computer Security Resource Center. [Database] https://csrc.nist.gov/glossary/term/information_security_program_plan

Newlove-Eriksson, L., Giacomello, G., & Eriksson, J. (2018). The Invisible Hand? Critical Information Infrastructures, Commercialisation and National Security. The International spectator, 53(2), 124-140. https://doi.org/10.1080/03932729.2018.1458445

Nielsen, J. A., Mathiassen, L., & Newell, S. (2014). Theorization and Translation in Information Technology Institutionalization: Evidence From Danish Home Care. MIS quarterly, 38(1), 165-186. https://doi.org/10.25300/MISQ/2014/38.1.08

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. European journal of information systems, 26(1), 1-20. https://doi.org/10.1057/s41303-016-0025-y

Niiniluoto, I. (1999). Defending Abduction. Philosophy of science, 66(3), S436-S451. https://doi.org/10.1086/392744

Paananen, H. (2023). Information security policy development: Considering the practices of making rules (JYU Dissertations 607) [Doctoral dissertation, University of Jyväskylä]. https://urn.fi/URN:ISBN:978-951-39-9297-2

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. Computers & security, 88, 101608. https://doi.org/10.1016/j.cose.2019.101608

Ransbotham, S., & Mitra, S. (2009). Choice and Chance: A Conceptual Model of Paths to Information Security Compromise. Information systems research, 20(1), 121-139. https://doi.org/10.1287/isre.1080.0174

Rashid, Y., Rashid, A., Warraich, M. A., Sabir, S. S., & Waseem, A. (2019). Case Study Method: A Step-by-Step Guide for Business Researchers. International Journal of Qualitative Methods, 18. https://doi.org/10.1177/1609406919862424

Rea, A., & Marshall, K. (2020). Information Security Research within the Information Systems Discipline: Analyzing, Categorizing, and Classifying the Historical Underpinnings and Theoretical Assumptions. AMCIS 2020 Proceedings. 13. https://aisel.aisnet.org/amcis2020/info_security_privacy/info_security_privacy/13

Reinking, J. (2012). Contingency Theory in Information Systems Research. In Dwivedi, Y., Wade, M., Schneberger, S. (Eds) Information Systems Theory. Integrated Series in Information Systems, vol 28. Springer. https://doi.org/10.1007/978-1-4419-6108-2_13

Sandelowski, M. (2000). Focus on research methods: Whatever happened to qualitative description ? Research in nursing & health, 23(4), 334-340. https://doi.org/10.1002/1098-240x(200008)23:4<334::aid-nur9>3.0.co;2-g

Schade, V. (2013). Successful Management of Mergers & Acquisitions: Development of a Synergy Tracking Tool for the Post Merger Integration. Anchor Academic Publishing.

Schneier, B. (2017). The Internet of Things Will Upend Our Industry. IEEE security & privacy, 15(2), 108. https://doi.org/10.1109/MSP.2017.39

Schultz, E., Proctor, R. W., Lien, M., & Salvendy, G. (2001-01-01). Usability and Security An Appraisal of Usability Issues in Information Security Methods. Computers & security, 20(7), 620-634. https://doi.org/10.1016/S0167-4048(01)00712-X

Simons, H. (2014). Case Study Research: In-Depth Understanding in Context. In P. Leavy (Ed.). The Oxford handbook of qualitative research. Oxford University Press.

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. Global journal of flexible systems management, 14(4), 225-239. https://doi.org/10.1007/s40171-013-0047-4

Singh, N., Krishnaswamy, V., & Zhang, J. Z. (2023). Intellectual structure of cybersecurity research in enterprise information systems. Enterprise information systems, 17(6). https://doi.org/10.1080/17517575.2022.2025545

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. Communications of the ACM, 49(8), 97-100. https://doi.org/10.1145/1145287.1145316

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. Information & management, 46(5), 267-270. https://doi.org/10.1016/j.im.2008.12.007

Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of Power: A Study of Mandated Compliance to an Information Systems Security "De Jure" Standard in a Government Organization. MIS quarterly, 34(3), 463-486. https://doi.org/10.2307/25750687

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International journal of information management, 36(2), 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Straub, D. W., Goodman, S., Baskerville, R. L., & Goodman, S. B. (2008). Framing the Information Security Process in Modern Society. Routledge. https://doi.org/10.4324/9781315288697-2

Subramanian, G., & Petrucci, C. (2021). Deals in the time of pandemic. Columbia law review, 121(5), 1405-1480.

Taherdoost, H. (2022). Cybersecurity vs. Information Security. Procedia computer science, 215, pp. 483-487. https://doi.org/10.1016/j.procs.2022.12.050

Thomas, G. (2011). A Typology for the Case Study in Social Science Following a Review of Definition, Discourse, and Structure. Qualitative Inquiry, 17(6), 511-521. https://doi.org/10.1177/1077800411409884

United Nations (n.d.). Sustainable Development Goals. [Website] United Nations. https://sdgs.un.org/goals

van Daalen, O. (2022). In defense of offense: Information security research under the right to science. Computer law & security review, 46, 105706. https://doi.org/10.1016/j.clsr.2022.105706

von Solms, B. (2001). Corporate Governance and Information Security. Computers & security, 20(3), 215-218. https://doi.org/10.1016/S0167-4048(01)00305-4

von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. Computers & security, 23(5), 371-376. https://doi.org/10.1016/j.cose.2004.05.002

Von Solms, R., Thomson, K., & Maninjwa, M. (2011). Information Security Governance control through comprehensive policy architectures. IEEE. https://doi.org/10.1109/ISSA.2011.6027522

von Solms, R., & (Basie) von Solms, S. (2006). Information Security Governance: A model based on the Direct–Control Cycle. Computers & security, 25(6), 408-412. https://doi.org/10.1016/j.cose.2006.07.005

Weill, P., & Olson, M. H. (1989). An Assessment of the Contingency Theory of Management Information Systems. Journal of management information systems, 6(1), 59-86. https://doi.org/10.1080/07421222.1989.11517849

Wæraas, A., & Nielsen, J. A. (2016). Translation Theory 'Translated': Three Perspectives on Translation in Organizational Research. International journal of management reviews : IJMR, 18(3), 236-270. https://doi.org/10.1111/ijmr.12092