TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

Ilona Ilvonen

Knowledge Security – A Conceptual Analysis

Julkaisu 1175 • Publication 1175

Tampere 2013

Tampereen teknillinen yliopisto. Julkaisu 1175
Tampere University of Technology. Publication 1175

Ilona Ilvonen

Knowledge Security – A Conceptual Analysis

Thesis for the degree of Doctor of Science in Technology to be presented with due permission for public examination and criticism in Festia Building, Auditorium Pieni Sali 1, at Tampere University of Technology, on the 29th of November 2013, at 12 noon.

Tampereen teknillinen yliopisto - Tampere University of Technology
Tampere 2013

Supervised by
Professor Mika Hannula
Associate Professor Nina Helander

Reviewed by
Professor Sirkka Järvenpää
Professor Aki-Mauri Huhtinen

ISBN 978-952-15-3186-6 (printed)
ISBN 978-952-15-3194-1 (PDF)
ISSN 1459-2045

Always be curious, always challenge, and always be ready to learn.

To the loves of my life: Ville, Matias and Sonja

ABSTRACT

ILVONEN, Ilona. 2013. 'Knowledge security – a conceptual analysis'. Department of Information Management and Logistics, Tampere University of Technology, Tampere, Finland.

Keywords: Knowledge security, Knowledge, Knowledge management, Information security management, conceptual analysis

Knowledge is an essential asset to companies in modern society. Knowledge is embedded in people, and it is nurtured and created through experience. Companies have taken actions to manage knowledge from such perspectives as its recognition, creation, sharing, and associated strategy. Although the security angle is mentioned in knowledge management literature, it is elaborated upon little in the knowledge management field. In contrast, information security management efforts approach the matter of a company's information assets from the security perspective, building security management processes that ensure the confidentiality, integrity, and availability of information. Although information security is in many cases considered a technical issue, the term can be interpreted as encompassing also knowledge. This study was conducted to determine what the term 'knowledge security' means, and how the fields of knowledge management and information security management can be brought together.

The study follows a conceptual analysis research approach to analysing the concept of knowledge security. Both theoretical and empirical material are used in the analysis: the theoretical analysis consists of an exploration of the uses of the knowledge security concept and examination of parallel concepts to it, and the empirical analysis examines how companies approach recognition and security of knowledge in their daily activities, whether or not they give those activities the name 'knowledge security'. In the final part of the work, the theoretical and empirical findings are synthesised, and a model for the concept of knowledge security is constructed.

Knowledge security is a process aimed at the security of knowledge that is embedded in the people working for a company and in their interactions. By recognising its important knowledge, a company can begin the process of managing and securing that knowledge. To be able to select appropriate security measures, the company needs to identify the threats that the knowledge faces. An information security framework with characteristics of integrity, availability, and confidentiality can be applied to the context of knowledge. The knowledge security model allows the characteristics of knowledge, the threats to knowledge, and the knowledge management initiatives to be examined in a coherent manner. This model can be utilised as a framework for further research and as a management tool in the corporate context.

TIIVISTELMÄ (ABSTRACT IN FINNISH)

ILVONEN, Ilona 2013. "Knowledge security – a conceptual analysis".
Tiedonhallinnan ja logistiikan laitos, Tampereen teknillinen yliopisto

Asiasanat: Tietämyksen turvaaminen, tietämys, tietämyksen hallinta, tietoturvallisuuden johtaminen, käsiteanalyysi

Tietämys on arvokasta varallisuutta nykypäivän yrityksissä. Tietämys on ihmisiin sitoutunutta, ja se kehittyy ja sitä luodaan kokemusten ja aiemman tietämyksen kautta. Tietämystä hallitaan yrityksissä esimerkiksi tunnistamisen, luomisen, jakamisen ja strategian näkökulmista. Vaikka tietämyksen turvaamisen näkökulma on mainittu tietämyksenhallinnan kirjallisuudessa, sitä ei ole tietämyksenhallinnan kentässä kovin laajasti otettu huomioon. Tietoturvallisuuden johtamisen lähestymistapa tietoon on turvallisuuden näkökulma, joka korostaa tiedon eheyttä, saatavuutta ja luottamuksellisuutta. Vaikka tietoturvallisuutta monesti pidetään lähinnä teknisenä asiana, voidaan käsitteen tulkita kattavan myös tietämystä. Tämä tutkimus selvittää tietämysturvallisuuden käsitettä, mitä se tarkoittaa, ja miten tietämyksenhallinnan ja tietoturvallisuuden johtamisen kentät voidaan yhdistää.

Tutkimus noudattaa käsiteanalyyttista tutkimusotetta. Analyysissa hyödynnetään sekä teoreettista että empiiristä materiaalia. Teoreettisessä analyysissa tutkitaan tietämysturvallisuuden käsitteen käyttöä, sekä tarkastellaan sen lähikäsitteitä. Empiirisessä analyysissa keskitytään selvittämään kuinka yritykset tunnistavat ja turvaavat tietämystä päivittäisessä toiminnassaan, välittämättä siitä kutsutaanko tätä yrityksissä tietämysturvallisuudeksi vai ei. Tutkimuksen lopussa teoreettinen ja empiirinen analyysi yhdistetään, ja tutkimuksen tuloksena rakennetaan malli tietämysturvallisuuden käsitteelle.

Tietämysturvallisuus on prosessi joka tähtää yrityksen työntekijöihin sitoutuneen tietämyksen turvaamiseen. Prosessi aloitetaan yrityksissä tunnistamalla yritykselle tärkeä tietämys. Jotta tärkeää tietämystä turvaavat toimenpiteet voidaan valita oikein, tulee myös tunnistaa uhkat, joita tähän tietämykseen kohdistuu. Tietoturvallisuuden johtamisessa käytettyä tiedon ulottuvuuksien, eheyden, saatavuuden ja luottamuksellisuuden, kehikkoa sovelletaan tutkimuksessa tietämyksen kontekstiin. Tietämysturvallisuuden mallia hyödyntämällä yritykset voivat tarkastella tietämyksen ulottuvuuksia, tietämykseen liittyviä uhkia, sekä tietämyksenhallinnan sekä turvaamisen keinoja yhtenäisenä kokonaisuutena. Malli tarjoaa siis työkalun yrityksen johdolle, ja sen sopivuutta työkaluna tulisi jatkossa testata.

ACKNOWLEDGEMENTS

Dissertation work, even though an individual journey of learning, cannot be completed without help. I have been fortunate to receive help from various people, and want to express my thanks to some of them here.

First of all I want to thank my advisors, Prof. Mika Hannula and Assistant professor Nina Helander. Mika, I thank for your support and advice during my studies. I feel I have had the freedom required to make my own choices concerning methodology, research questions, and theoretical field, as long as I have had good reasons for them. I feel you have trusted in me to find my way and make informed choices, and this trust has empowered me to explore and "try my wings" in research. Yet, in every phase of the process, when I have felt lost or in need of encouragement and guidance, I have received it from you promptly. You have seen in me the potential for a doctoral student early on in my studies, and I thank you for allowing me to grow in the process and work independently.

An equal amount of thanks belongs to my other advisor, Assistant professor Nina Helander. I thank you for the encouragement, critique and friendship you have offered during these years. Many a conversation with you has begun with the theme of "I don't know whether I should do this or that", and ended with a clear idea of which is the better choice for me. The frustrations and insecurities that are inevitable in the process of finding the right path toward a finished dissertation have been substantially alleviated by the calm and insightful feedback from you.

I wish to thank the pre-examiners of this dissertation, Prof. Sirkka Jarvenpaa and Prof. Aki-Mauri Huhtinen for constructive and encouraging comments on the manuscript. Your feedback has pointed out where it could be improved, but also encouraged me to pursue this line of research further after this dissertation. The comments have been valuable in finalizing the dissertation.

I have had the opportunity to work with the greatest colleagues around me at research center NOVI in TUT. Especially I thank Dr. Vilma Vuori for collaborating with me in joint research paper projects that have been a wonderful way of sharing ideas and also sharing the pressure of writing. The co-authored papers with you have been my school to joint writing. I thank you also for the peer-support in writing up the dissertation, your efforts in finalizing your work were an inspiration to me, even if mine took a while longer.

I also wish to thank my closest colleagues Dr. Marianne Kukko, M. Sc. Pasi Virtanen, M. Sc. Jussi Myllärniemi and M. Sc. Terhi Yliniemi for your friendship and support that you have given me over the years. Many a laugh has been enjoyed together over lunch

or coffee (or tea). The ups and downs of research, teaching, raising children and building or renovating, among many other topics, have been shared with you, and I feel grateful for all the moments together. At times there has been stress, pressure and difficulties, but I can have counted on support and help from all of you. I wish to be of equal support to you when you need it, and hope our collaboration and friendship will continue also in the future.

I thank the department head, Prof. Samuli Pekkola for allowing me time to work on this dissertation, and offering advice in the research process. The department of information management and logistics has been a great place to work. In addition to the people mentioned above, many others have contributed to the fun and relaxation that takes place over morning or afternoon coffee. Although it may seem odd to emphasize the role of the shared brakes, this is what has substantially helped me in working with this dissertation. Although I have been alone in writing, I have had colleagues around me even if we have not effectively been working together. Shared humor brings people together, and relieves the stress that intensive research many times causes.

This dissertation is quite theoretical in nature, but it would be even more so if I had not had the opportunity to enter some companies and interview their representatives. I would very much like to thank all of you with your names, but because I have promised not to disclose the companies I have interviewed, I need to just thank you anonymously: thank you for allowing me to come and ask you difficult questions! I hope we can continue collaboration in the future.

Besides working on my dissertation, there have been other, more important, elements in my life too. I thank all of my friends for being there for me, and sharing the joys and challenges of life with me and my family. I may have not always been the best of company because of the strains of work, but regardless of this, you have supported and encouraged me, and offered me other things to think about. Be it a birthday party or meeting over dinner, I always enjoy the company of you all.

Especially I want to thank Dr. Satu Jumisko-Pyykkö for offering your friendship and support. I have very much enjoyed the family outings we have shared, and the travels we have done together. You have been an inspiration to me as a researcher, and your comments on the manuscript with the eyes of someone outside my field were valuable.

In addition to friends, I have received a lot of support and encouragement from my family. I thank my sisters, Irmeli Hirvensalo and Irina Tornikoski, for your support and (usually) gentle instruction on life from early on. You have taught me many valuable skills in life, reading not the least important. Later on you have provided me with challenging discussions, yet loving support. During this dissertation work you have been one link to the corporate world, sharing your experiences with me.

I want to thank my parents, Inkeri and Iiro Hirvensalo, for always being there for me, yet raising me to take care of myself. Father, you have been the loving and caring person in my life, who made me believe I can do anything I want, whether it is to drive a train, play music or become a researcher. You have never questioned my ability to do something, and you yourself show the example by doing many activities you find interesting and rewarding. You find time to support, encourage and help not only your children, but a large circle of friends as well. You are an inspiration to me.

Mother, you have always offered encouragement, support, help and comfort when I have needed it. You have also inspired me with your example, by being ambitious in your work, by educating yourself, and by earning your doctorate. I feel that you, too, have always supported me in whatever it is that I do, and want to do everything you can to help me in the way. I thank you for commenting on the manuscript, but also on your gentle support and listening throughout this process. You have not voluntarily offered advice, but you have always had some advice to give when I have asked for it. I hope I can be the same kind of support figure for my children.

I thank my in-laws, Pirjo and Tenho Ilvonen for your support over the years. You have been kind enough to take me in as a part of your family. Your support and encouragement has been great, as well as your concrete help in caring for our children and pets when we have needed your help.

Last, but not certainly least, I want to thank the people closest to me: my husband Ville, our son Matias and daughter Sonja. Ville, I thank for your love and the support you have given me. Words cannot describe how much I love you, and how much I appreciate all the things we share together. We have a great life together, and I'm sure we will share a lot more over the years to come. Matias and Sonja, thank you for being you, and reminding me to focus on what is the most important: being with the people we love.

At home in Tampere 30.10.2013

Ilona Ilvonen

Table of contents

List of figures

List of tables

1 Introduction

This book presents a doctoral thesis that focuses on knowledge security. This introductory chapter presents the background for the study and introduces the research questions. Also, the scope of study is introduced and discussed. The discussion proceeds to explanation of the research approach and strategy, before the chapter concludes with presentation of the research process and the structure of the work.

1.1 Background and motivation for the study

Knowledge, people's accumulated experiences and abilities or insights, is an essential asset to companies. This asset has been widely studied from various perspectives, including those of its management (Choo 1996, Hislop 2005, McInerney & Day 2007, Maier 2010), creation (Nonaka 1994, Nonaka et al. 2000, Scheepers et al. 2004, von Krogh 2009), and sharing (Ipe 2003, Riege 2005, Rangachari 2009, Suppiah & Manjit 2011). The message of many knowledge management (KM) studies is that knowledge, when created, fostered, managed, and shared well, can provide a company with improvements in performance (Nold 2012).

The field of knowledge management is a multidisciplinary one (Argote et al. 2003, Maier 2010, p. 34). Studies approach managing knowledge, for example, from the perspective of organisational culture (e.g., Potter 1989, Nonaka 1991, Rai 2011), information systems (e.g., Wilkins et al. 1997, Alavi & Leidner 2001, Thierauf 2001, von Krogh 2009), strategic management (Prahalad & Hamel 1990, Choo 1996, Spender 1996, Ma & Yu 2010), and intellectual capital (e.g., Bontis 1998, Nahapiet & Ghosal 1998, Schiuma 2012). These disciplines each bring their own perspective on what knowledge is and on how it can be managed and utilised to a company's advantage. Although knowledge management is a multidisciplinary field, many studies remain tied to a single perspective or background theory, though combining many of them might bring more fruitful results.

In intellectual capital literature, the management and measurement aspects are especially prominent (Bontis 1998, Schiuma 2012). The word 'capital' in this term refers to an asset that has measurable monetary value and that can be used as one component in production of goods and services. Intellectual capital is commonly divided into three categories: human capital, structural capital, and relational capital (Bontis 1998). Human capital refers to the employees' competencies and knowledge, structural capital involves business processes and documented information stored in databases, and relational capital refers to customer and stakeholder relationships and brands (Seetharaman et al. 2002, Sillanpää et al. 2010). The second type listed, structural capital, includes the intellectual property rights (IPR) of the company, and

these are often discussed in the context of protection (Baughn et al. 1997, Sanyal 2004). Relationship capital too is considered important to protect, since strong relationships form a basis for many business opportunities (Baxter & Matear 2004, Bueno et al. 2004). Finally, human capital is considered equally important as a part of intellectual capital alongside structural capital and relational capital. The protection perspective expressed is that of losing knowledge upon retirement (De Long 2004), but retirement is surely not the only risk threatening the human capital of a company – for example, job rotation can also create risks (Brunold & Durst 2012). The protection-oriented approach to intellectual capital overall is still emerging, with, for example, the insurance industry interested in the topic of protecting intellectual capital (Mäenpää & Voutilainen 2012).

Knowledge is a part of human capital, since knowledge is to a large degree bound up in people who possess the knowledge. From the point of view of a company, all capital assets, physical, monetary, and intellectual, should be protected through active security efforts. All of these are among the factors on which business is based on. In today's world, the products themselves are quite often intangible, which makes the intangible factors of production the most important ones. Many companies are on a path of increasing the proportion of knowledge work in their operations (Blackler 1995, Assudani 2009) while the share of physical work done by people is decreasing. The emergence of the knowledge management field is in part a consequence of this development: knowledge has an increasingly important role in companies.

Knowledge can be regarded as one part of the complex entity that usually is referred to by the term 'information'. A terminological difficulty in the English language arises from the lack of an umbrella term that could encompass all of the diverse dimensions to information and knowledge. In the native language of the author, Finnish, such a term, 'tieto', does exist. This word is used as a general expression to denote, for example, data stored in databases, information provided by books and manuals, and knowledge that people gain – along with their experiences in interpreting and using the data and information at their disposal. In the English language, in contrast, the word 'information' is many times used as a general expression in this sense, but the term also has a more specific connotation. This overloading of the term can sometimes cause difficulties in understanding what is meant when it is used in a given context. In this study, the relationships among these terms are discussed in greater depth in Section 2.1.

Thierauf (2001) presents a hierarchical categorisation of, from bottom up, data, information, and knowledge. The field of information security concentrates mainly on the two lower levels. Information security has received a fairly large amount of attention, especially from the technical and management perspectives (von Solms & von Solms 2004a). Information security culture and behaviour have also been studied a lot, but still the focus has been on the use of and adaptation to technical security solutions (Johnston & Warkentin 2010, Siponen & Vance 2010). The security perspective is seldom brought into discussion of knowledge (Ryan 2006a, Shedden et al. 2011), even though it can be argued that security is one very important aspect of the efficient use of knowledge

(Maier 2010). If information security does not consider knowledge, perhaps a separate concept of knowledge security (KS) is needed to complement the security discussion. Concepts are tools for managers and scientists who aim to understand and develop the phenomena that occur in companies. The concept of knowledge security may open new perspectives for management of knowledge that is important to a company.

Even though the concept of knowledge security is not widely used (Desouza 2006, Ryan 2006b, Shedden et al. 2011), companies do secure knowledge in their own chosen ways. They put effort into creating security cultures that foster knowledge, prepare initiatives for knowledge retention in awareness of retirement, and encourage their employees to share important knowledge. Whether a company does this for security purposes or for other reasons may affect the outcome of the activities. If knowledge is shared in the company to make the work more effective (Barachini 2009), the sharing may or may not support the securing of important knowledge against, for example, employee turnover or leaks to competitors.

What the security point of view on knowledge is, how it affects the other approaches to knowledge, and what benefits it could bring to companies are questions that the author has found perplexing over the years. Focusing the research on a single phenomenon that can be tackled within one dissertation has led to analysis of the concept of knowledge security. The viewpoint of security here seemed to be largely absent from current literature, at least in the eyes of the author. Many authors mention that protecting knowledge is important (Gold et al. 2001, von Krogh et al. 2001, Maier 2010). However, their studies have not adequately addressed how the protection of knowledge should actually be implemented and how companies perform it. Some studies merely mention this area as difficult and challenging (Gold et al. 2001, Donate & Canales 2012). The topic chose itself by appearing fresh, promising, and to be an area in which there is a chance of finding common ground among several areas of research.

Although the information security management literature has long emphasised that all company information, knowledge included, needs to be secure (von Solms & von Solms 2004a, Peltier et al. 2005), scientific attention has been focused mainly on security of information systems (Anderson & Agarwal 2010). The motivation for this study comes from widening the scope of research and from bringing the fields of knowledge management and information security management into the same scientific discussion. Described briefly, the motivation for the study is to argue that the concept of knowledge security should be adopted in scientific discussion.

1.2 The research objective and scope of study

The objective of this study is to analyse the concept of knowledge security. The concept is used by only a few authors (Desouza & Vanapalli 2005, Desouza 2006, Ryan 2006b, Ryan 2006c, Desouza 2007, Shedden et al. 2011), but the assumption of the author of

this study is that there are, on one hand, existing activities that could be covered by the term 'knowledge security' and, at the same time, demands for structured activities called knowledge security. The primary ontological research question for this study is this:

What is knowledge security?

The question is answered both theoretically and empirically. The question can be further broken down into sub-questions:

a) How are knowledge security and related concepts defined and referred to in contemporary literature?

A systematic literature review is performed to discover the use of the concept of knowledge security and the contexts and discussions in which that concept is or could be used. Related topics, such as knowledge risk, knowledge protection, security awareness, security culture, security policies, and knowledge management, are reviewed. The literature streams of information security management and knowledge management are both analysed, for a broad perspective on the field of study. Preliminary empirical material is used to guide the literature review.

b) How do companies secure knowledge?

The research task is focused on the existing practices of addressing knowledge in security efforts, with the task being to discover the views of existing companies and find out how they believe they are handling knowledge security. Also, the relationship between knowledge management and information security initiatives in case companies is examined, as sometimes these fields can be seen as in conflict with each other. Although the question is ontological, not normative, the answer inspires also discussion of how companies could keep knowledge secure even if they are not currently doing so.

As introduced above, the concept under study is knowledge security. Desouza (Desouza & Vanapalli 2005, Desouza 2006) and Ryan (2006a, 2006b, 2006c) introduced the concept in scientific fora, although calls for research into human aspects of information security were made earlier (e.g., Majchrzak & Jarvenpaa 2004). The main arena for scientific discussion of knowledge security has been the information security journals, although some articles can be found also in knowledge management journals.

Knowledge as a concept can be seen as part of the above-mentioned concept hierarchy of data, information, and knowledge. Knowledge is *embedded in people and their experiences*. In a business context, this necessitates widening the scope from examining individual people also to considering communication between people, since knowledge needs to be exchanged by people in order for their company to do business.

Accordingly, knowledge is examined from both the individual's and the collective perspective (von Krogh et al. 2001, von Krogh 2009).

Desouza (2007) ties the concept of knowledge security closely to that of intellectual assets. Intellectual assets, also called intellectual capital, are referred to as the knowledge and knowing capability of a company (Nahapiet & Ghosal 1998). More specifically, this set can be defined as the intersection of a company's human, structural, and relational capital (Bontis 1998). In this study, the focus is placed on human capital especially, since the interest is in security of the knowledge embedded in people. Structural capital and relational capital are also largely based on people and their interactions; therefore, it is reasonable to state that knowledge security is linked to intellectual capital as a whole. However, theories of intellectual capital are not given the focus in this study; instead, they may be one context for future study of knowledge security.

Figure 1 illustrates the key concepts of this study, their relationships, and the context of the study. The work brings together the fields of knowledge management and information security management, and, from a broader perspective, it draws in the knowledge-based view and information systems literature. These fields share a common ground, created from the combination of knowledge management and information security management. The study contributes the knowledge management perspective to the information security field and the concept of security to the knowledge management field.

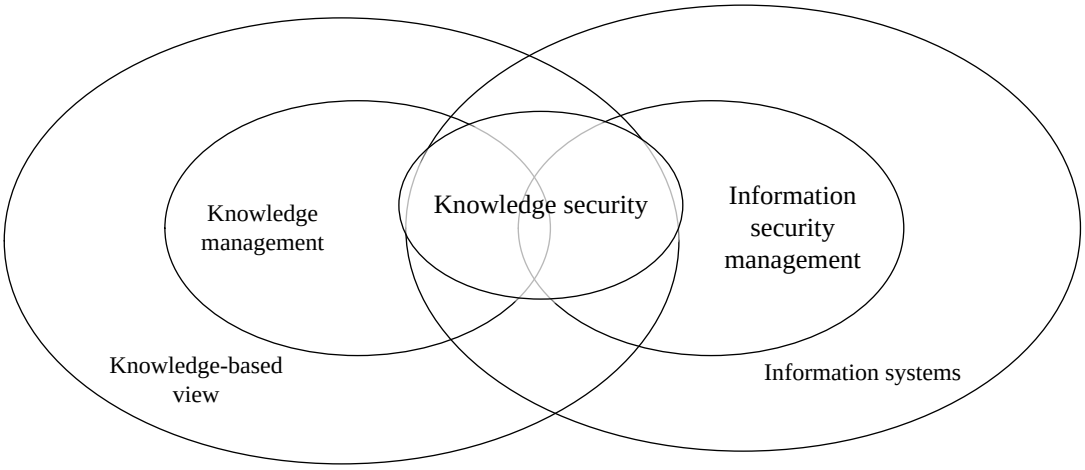

Figure 1: The key concepts and the fields of study

Knowledge can be regarded as an important resource and asset for a company (Spender 1996), and this knowledge-based view, on the left-hand side in Figure 1, is a starting point for this study. From this knowledge-based angle, knowledge is examined from the management standpoint, and the potential uses for the knowledge determine the knowledge's value. Knowledge creation and knowledge sharing as parts of knowledge management work are addressed from the perspective of security – i.e., what kinds of

security considerations are needed when new knowledge is created and when people make decisions to share knowledge.

The main setting for the emerging scientific discussion on knowledge security has been the field of information security management, on the right in Figure 1. This field belongs to the larger discipline of information system science. Forming a starting point for this discussion are the information security management models that call for security of all information assets, including those that reside within the employees of a company (Whitman & Mattord 2003, von Solms & von Solms 2004a, Werlinger et al. 2009). The security management approach to information entails recognising the important information, identifying the threats this information faces, implementing security controls to counter those threats, and systematising all of this in a security management process (Whitman & Mattord 2003, Peltier et al. 2005). This security-oriented approach is extended to knowledge in the present work.

The second research question, about how companies keep knowledge secure, has a practical element. For example, in the field of strategic management, the practical dimension of strategy and the people implementing strategy is discussed (Mantere 2005, Mantere & Vaara 2008, Jarzabkowski & Spee 2009). Although the research questions are positioned at the strategic level, and strategy-as-practice as a research field therefore has similarities with the work in this study, the main theoretical grounding of the study is in information systems and knowledge management. Although it would be a viable and interesting line of attack to extend the focus of this study to the strategy-as-practice field, the choice has been made to leave it beyond the work's scope, since it would substantially widen the study. The term 'strategy' is present in this dissertation as used in knowledge management strategy or information security strategy. These are closely connected to strategic management and thus also the strategy-as-practice field. This connection is acknowledged but not further explored in the study, since the focus here is on finding a definition for 'knowledge security'. At the end of the dissertation, future lines of study are discussed, the connection to strategic management being one of them.

The context for this study is companies. The term 'organisation' is often used to refer to companies and corporations (see, e.g., Morgan 2006, p. xi). However, the term is more general and encompasses public organisations too. Companies are organisations that are dependent on knowledge for success in business (Grant 1996) and that are formed to conduct business and create profit for their owners (Penrose 1995, Ministry of Justice 2012). There is little difference between companies and other organisations in the need for security of knowledge, but the scope of this study is limited to companies, since empirical material has been gathered only from companies. At the end of the study, the generalisability of the empirical results to other organisational contexts is discussed and further work in other types of organisation is recommended.

1.3 The research approach and strategy

This section of the chapter discusses the philosophical choices and research approach. The research approach, conceptual analysis, is introduced alongside the research strategy that was followed in implementation of the approach.

1.3.1 The philosophy of a concept

This study examines a new and emerging concept. Before the research approach itself is considered and strategy and methods can be discussed, a brief introduction is needed to explain what is meant by the term 'concept' in the context of this study.

A concept is a construct that has the dimensions of a term, a word (or a combination of words, as is the case in this study), the phenomenon that is described with the term, and the meaning or meanings that the term carries (Niiniluoto 1984). These are illustrated in Figure 2.

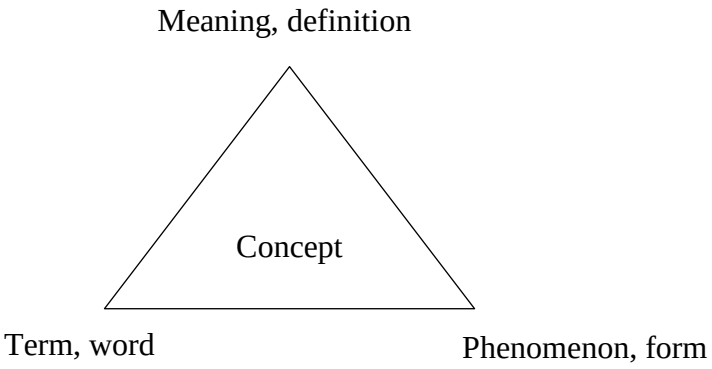

Figure 2: A concept as a construct, based on the work of Niiniluoto (1984, p. 118)

There are many, quite different, approaches to what exactly a concept is, but this mediaeval semiotic triangular approach illustrated in Figure 2 brings out the complex nature of a concept well. The term that is connected to a concept may be connected to other concepts as well; i.e., the same word can be connected to many meanings that are, in turn, connected to more than one phenomenon. Also there are degrees of depth to a concept, and whether a given form or phenomenon corresponds to a definition depends on the detail of the definition.

For example, the term 'fish' can be used to describe a creature living in water. The meaning of the word 'fish', the concept of fish, may have several variations, depending on who is using the term, for what purposes (Wilson 1963). The debates connected to concepts are debates about definition. Here, the debate on what kinds of creatures are to be classified as fish is a debate on definition. Depending on the characterisation, a shark, a whale, a starfish, and a lobster may each be classified as fish or as something

other than fish. If the only definition given is that a fish is a creature that lives in water, all of the above are fish according to that definition. However, when we add more characterisations to the definition, such as that a fish breathes with gills under the water and is cold-blooded, we exclude the whale from the list. The ability to swim more or less prunes the starfish from the list, and the feature of having fins leaves the lobster out. A concept is thus a construct of a name and a definition for a phenomenon: what categorises a creature as a fish depends on the definition of the term 'fish'.

Analysis of a concept requires analysis of the connections among the name, the phenomenon, and the definition for it. There may be different names for a phenomenon, and there may be several definitions for those names, just as there might be different definitions for a phenomenon. In the case of an emerging concept, careful consideration needs to be given to all dimensions of the concept. The name of the concept under research in this study is 'knowledge security'. The goal is to find the phenomenon behind this name, define it, and also find potential different names for the phenomenon or parallel phenomena. The main unit of analysis, however, is the term knowledge security.

The concepts and connections under examination in this study are further illustrated in Figure 3. The security management elements of threat identification and assessment, security controls, and the overall idea of a security management process are applied to the context of knowledge. Knowledge, its management, and security management are considered to be concepts close to that of knowledge security.

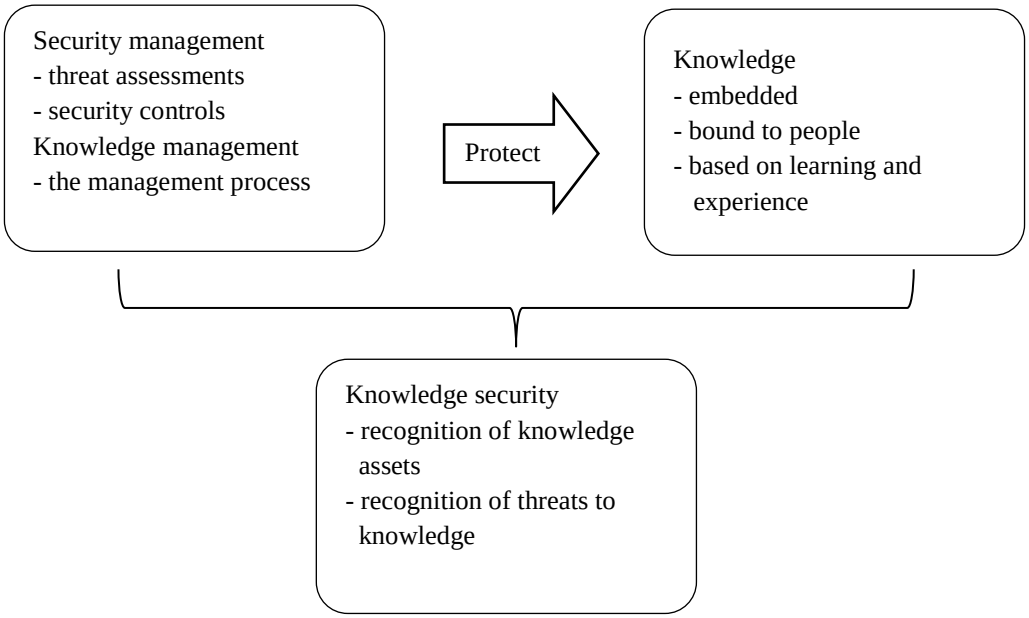

Figure 3: Relationships among the key concepts

In Figure 3, knowledge security is considered a phenomenon that emerges from the process of implementing security management efforts aimed at protecting knowledge.

One assumption behind this study is that knowledge security is a result of active knowledge protection in a company. This process can be systematised and managed through understanding of the dimensions and drivers of the concept. The study proceeds from the assumption that recognition of knowledge assets, recognition of threats, and selection of protective measures are key elements of knowledge security.

1.3.2 Research philosophy

Every piece of research springs from the questions and assumptions of the researcher. This study is no exception: the research questions, discussed in Section 1.2, reveal underlying basic assumptions of the researcher. In this case, the assumptions have to do with the nature of knowledge and the possibilities for creating scientific knowledge about the research topic (i.e., the ontology and epistemology of this research). Burrell and Morgan (1979) distinguish between the subjectivist and objectivist approaches to social science, and this widely applied distinction is useful also for the present study. They identify four distinct 'axes' along which a piece of social science research can be analysed. These are illustrated in Figure 4.

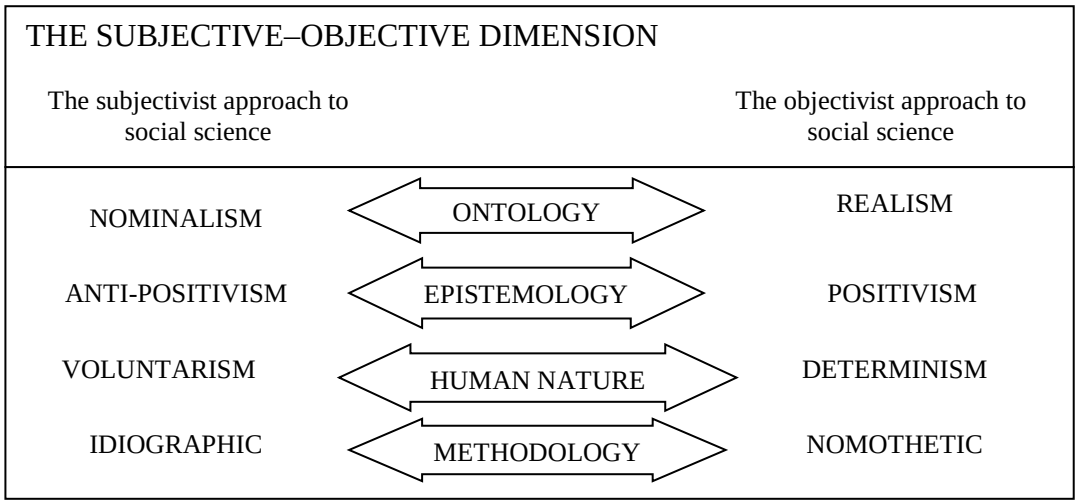

Figure 4: The subjective and objective dimensions of social science (adapted from Burrell & Morgan 1979)

The ontological continuum is between nominalism and realism. Nominalism is rooted in the assumption that the social world external to individual cognition is made up of nothing more than names, concepts, and labels that are used to structure reality. The nominalist does not admit to there being any 'real' structure to the world that these concepts are used to describe. A realist, in contrast, states that the structures of the social world are hard and tangible, whether or not they are labelled and perceived (Burrell & Morgan 1979). On the ontological axis, this study is closer to the realistic end of the continuum, since the analysis of a concept referred to as knowledge security implies that such a construct truly exists and can be empirically found in companies.

The epistemological extremes of social science are positivism and anti-positivism, or hermeneutics. These approaches refer to the way the researcher sees reality and thinks it can be explained. Positivism is a philosophical system recognising only that which can be scientifically verified or which is capable of logical or mathematical proof. This means that a positivistic approach aims at verification and proof of the phenomena under research. Anti-positivism, on the other hand, argues against the utility of a search for laws or underlying regularities in the social world. The researcher's position as a neutral observer, fundamental to the positivist approach, is deemed impossible, since the social world is relativistic and can only be understood from the point of view of the individuals who are directly involved in the activities under study (Burrell & Morgan 1979).

Positivism is a research philosophy usually present in natural sciences such as mathematics and physics. The main idea is that all true scientific knowledge is based on measured facts. Empirical material is gathered to verify or disprove scientific hypotheses, and the analysis methods are usually statistical (Saunders et al. 2009). Positivism aims to produce objective facts about the world. Reliable and valid measurements are sought, for generalisability of the empirical results: positivistic studies should be replicable – the same results and interpretations should be reached if another researcher were to repeat the study. The aim of anti-positivism, or hermeneutics, on the other hand, is understanding of phenomena, and interpretation has a very large role (Metsämuuronen 2005). Unlike in positivism, no objective truth can be reached in this view, and the understanding of the phenomena may change with the person performing the analysis.

As Olkkonen (1993) introduces it, the research history in industrial management features both positivistic and hermeneutic studies. The world of technology has its roots in natural sciences and has a positivistic tradition, while management science was born of the social sciences and so has a hermeneutic tradition. With both sets of background, researchers can choose the philosophy and methods they find appropriate for the research problem at hand (Olkkonen 1993).

The characteristics of knowledge that can be explored via the knowledge research determine the research paradigm to be used. This study employs a paradigm that draws mostly from the management research tradition, and thus has more hermeneutic than positivistic characteristics. Burrell and Morgan (1979) argue that also within the social sciences there are studies that approach the topic from a realist and positivistic angle. Although social phenomena cannot be measured as accurately as physical objects, the studies are still designed for broad generalisability and objectivity. The hermeneutic, subjective end of the continuums on Figure 4, on the other hand, places stress on the unique nature of social objects and eschews a demand for general rules. When viewed in the above analytical framework, this study can be seen as lying at the middle of the continuum, at neither the far subjective nor the objective end. The concept under study is seen as a construct of knowledge embedded in people and the actions that companies

take for security of that knowledge. Since knowledge is an individual-level attribute, the treatment of knowledge cannot be studied with full objectivity. The use of multiple interviewees creates some room for generalisability of the results, but it must be acknowledged that the researcher's interpretations have a large role in the empirical part of this study.

1.3.3 The research approach

A study's research approach is traditionally chosen on the basis of the kind of knowledge the researcher expects to gain with the study or what kind of question the researcher wants to answer (Maxwell 1996, p. 15). Within the framework of Burrell and Morgan (1979), the approach is chosen in line with how the researcher sees human nature: as a deterministic entity that is a part of a structure or as a voluntary unit. Since this part of the framework is perhaps more specific to social sciences, wherein people are the subject of study, it is better to find another perspective for the selection of approach. In this study the objective is to analyse the concept of knowledge security. In the case of an emerging concept, the analysis can also be called exploration, and for explorative studies a qualitative research approach is considered more suitable than a quantitative one (Maxwell 1996, p. 19). However, describing the research approach simply as qualitative does not provide adequate information about the approach used here.

This piece of research is a conceptual analysis. Puusa (2008) argues that conceptual analysis is an approach suited primarily to theoretical studies. She also stresses that conceptual analysis is an important part of many studies but that in those cases it has the role of a method more than that of an approach. In this study, both roles are taken. Although this study does have an empirical component, the role of that portion is to complement and add depth to the theoretical analysis of the concept. In its approach, the way this study is conducted as conceptual analysis can be characterised as an exploration of the uses and definition of the concept of knowledge security.

The last continuum in the framework depicted in Figure 7 involves methodology. Idiographic methods are aimed at the understanding of a phenomenon, and nomothetic methods at generalisable laws of phenomena. The methods chosen in this study are qualitative in nature and aimed at the understanding of a concept, so the methods used are closer to the idiographic end of the spectrum. The theoretical parts of the conceptual analysis are completed through a literature review. In the empirical work, the data collection method is the semi-structured interview and the analysis method content analysis. The methods are discussed in detail at the beginning of the chapters in which they are applied.

Puusa (2008, p. 43) introduces an eight-step model of conceptual analysis that is designed for use in business and management studies. That model takes into account the

fact that most concepts used in this field are of an abstract nature and can have multiple uses and definitions. The model is illustrated in Figure 5.

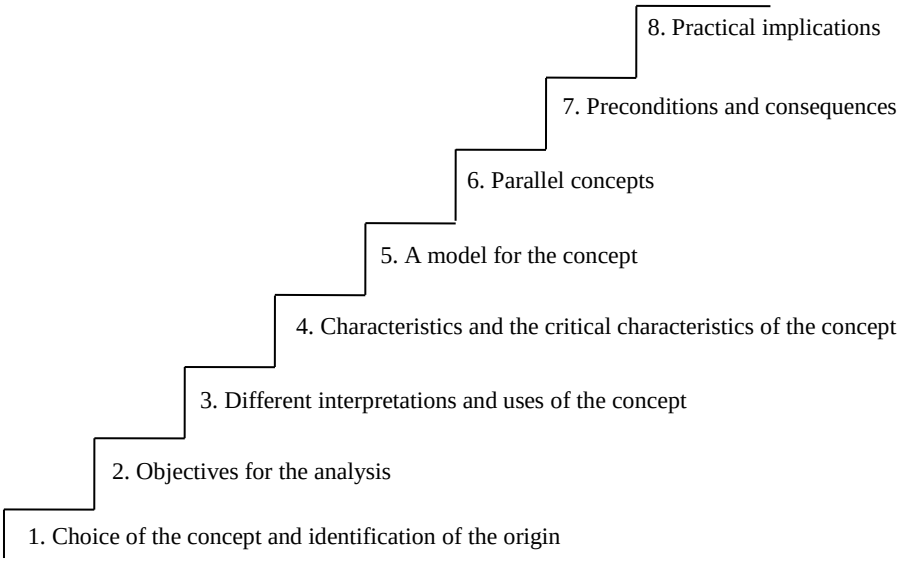

Figure 5: The phases in conceptual analysis (Puusa 2008)

Performing analysis following the eight steps illustrated in Figure 5 is fairly straightforward. The first step in the model is the choice of concept. However, as has been noted above, most concepts in the field of business and management are abstract in nature, and it is sometimes difficult to distinguish between concepts and then come up with the most appropriate one for the particular research at hand. The second step in the analysis is to set the objective. In this case, the objective is to find a definition for a concept. The third step is to find different interpretations and uses of the concept, by, for example, systematically searching for the uses seen in the literature. The fourth step is to identify the characteristics of the concept. In this phase, all of the various interpretations and definitions are analysed and key identifiers and characteristics of the individual definitions are compared. The outcome of this analysis is then built into a conceptual model in the fifth step of the analysis process. (Puusa 2008)

Although performed to some extent in tandem with the larger process, examination of parallel concepts and their points of interaction with the concept under study forms the sixth step of the model in Figure 5. In this stage, all concepts that interface with the concept under study are examined and the connections and distinctions between concepts are thoroughly discussed. This ensures that after the choice of concept and after in-depth concentration on a single concept, the researcher goes back and looks at the broader picture. After this comparison, the seventh step of the process is a natural progression, to description of the prerequisites for the concept under study and of its consequences. This aids in further clarifying the distinction between preconditions for the concept and characteristics of the concept: in which conditions can the concept exist, and in these conditions, what characterises the concept? (Puusa 2008)

The eighth and last step in the conceptual analysis process described in Figure 5 is to discuss the practical implications of the analysis. In this phase, the researcher describes how the concept is used in practice, how it can be measured, and what this implies for the practitioner (Puusa 2008). Puusa's model depicts the steps as a process that requires completion of the previous phase before the next step is begun.

Another commonly used model for conceptual analysis is presented by Rodgers (1989), according to whom the phases of evolutionary concept analysis are 1) choice of concept; 2) planning of the research setting, sample, and acquisition of data; 3) data acquisition (characteristics, supplementary concepts, references, preconditions, and consequences); 4) identification of parallel concepts; 5) data analysis; 6) comparison between disciplines; and 7) identification of a 'showcase sample' for the concept, if possible. These steps are not a linear progression; they are parallel activities in the analysis. They are shown in Figure 6.

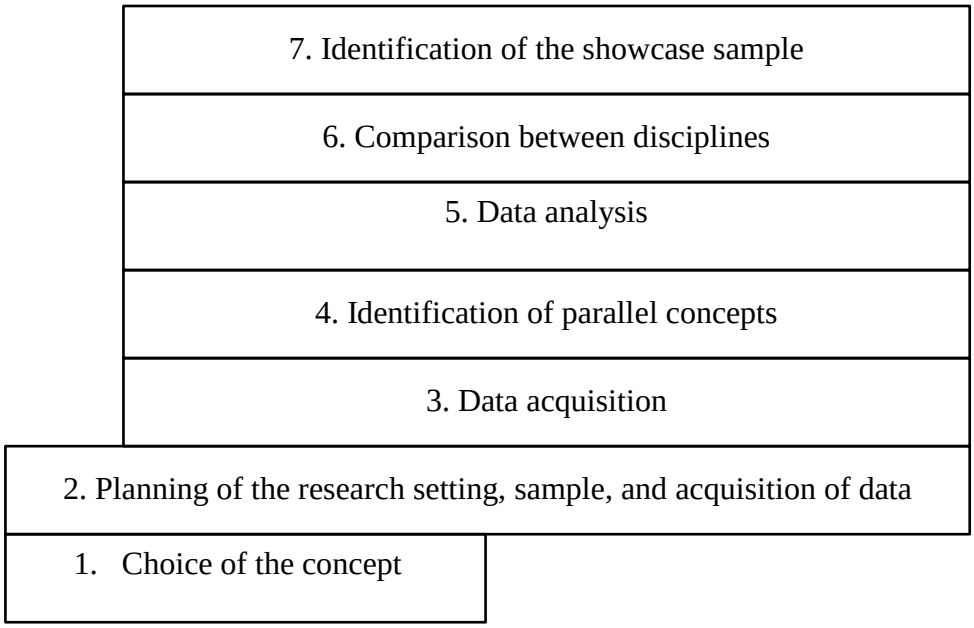

Figure 6: The steps in conceptual analysis according to Rodgers (1989)

The first two steps in Figure 6 are assumed to take place before the rest of the steps, which are described as taking place in parallel with each other. Although the steps can be seen as parallel, there are some timing dependencies, since the choice of concept is a trigger for the whole analysis process and the planning needs to precede the other phases. After initial planning, however, the conceptual analysis process can be parallel and iterative, as illustrated in the figure.

This study follows a conceptual analysis model that is constructed as a synthesis of the above models of Puusa (2008) and Rodgers (1989). While some steps in the model used are common to those in the source models, the order and description of the steps are

different. The way this study is conducted bears a resemblance to both models but is not very similar to either of them. The model employed is presented in Figure 7.

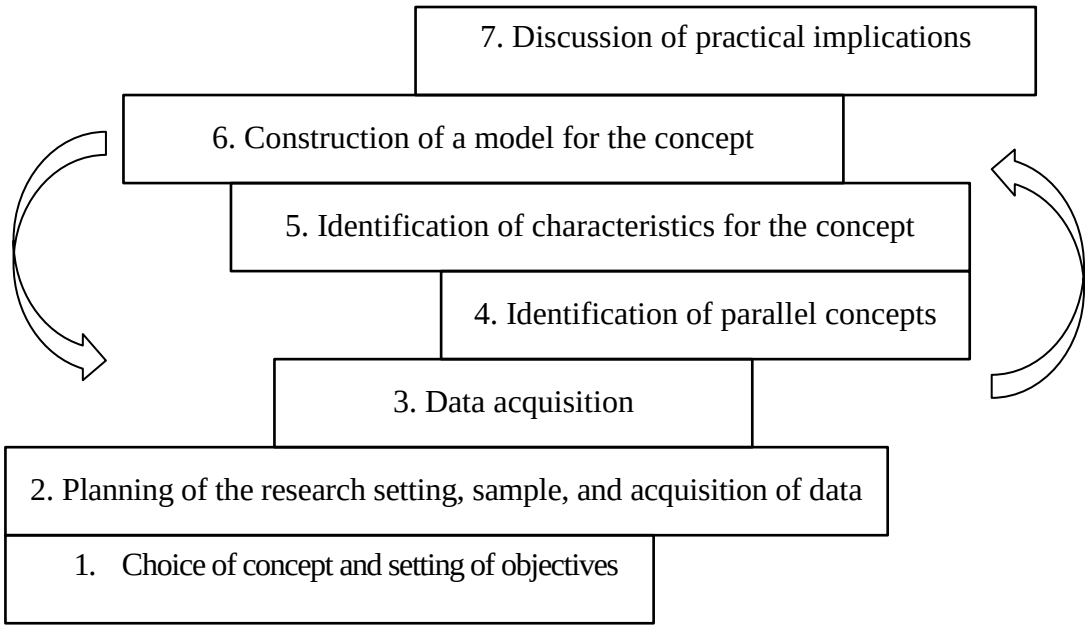

Figure 7: The steps in the conceptual analysis in the present study

In Figure 7, the steps of conceptual analysis are depicted as partially iterative and parallel. The main difference between the models of Puusa (2008) and Rodgers (1989) and the model used in this study lies in the iterative nature of the steps. Puusa (see Figure 5) describes the conceptual analysis process as a linear process that progresses in a certain order toward the end result of a model for a concept and its practical implications. The model by Rodgers (in Figure 6) emphasises the parallel execution of the various steps. However, it does not include the development of a model or emphasise the strong connection of a concept with practice. Combining the advantages of the two models, the model used in this study (as shown in Figure 7) includes parallel and iterative steps that accumulate understanding of the concept. The aim is creation of a model for the concept and discussion of its practical implications.

1.3.4 The research strategy

In this study, the implementation of a research approach in specific action steps is called a research strategy. In the following discussion, the steps of conceptual analysis explained above are described in more detail to present and detail the strategy of this research.

In phase 1 of conceptual analysis as described in Figure 7, the choice of the concept under study is made. In this study, the choice of concept was born of the background of the author: the middle ground between information security management and

knowledge management drew interest. The concept came up in some articles, and studying it seemed more and more interesting and relevant over time.

The design of the research setting underwent a great deal of iteration during the research process. A dissertation process is also a process of maturation for the candidate, and the present study proved no exception. The interest came to focus on the concept of knowledge security over time. Since the first draft of the research plan, the scope of study has shifted from information security policies and strategies in networks to the concept of knowledge security. Amidst seemingly constant changes in research focus, the only constant seemed to be the concept of knowledge security. This is why it can be said that the topic chose itself, by emerging from a cloud of interesting research topics.

The final research design was chosen when the first primary interviews were agreed upon. The literature review was carried out while changes were still being made in the research focus and had an impact on the final empirical research setting. A more detailed illustration of the steps in the conceptual analysis performed in this research is supplied in Figure 8. This illustration is a simplification of the process, but it illustrates the temporal order of the activities in relation to the phases of conceptual analysis.

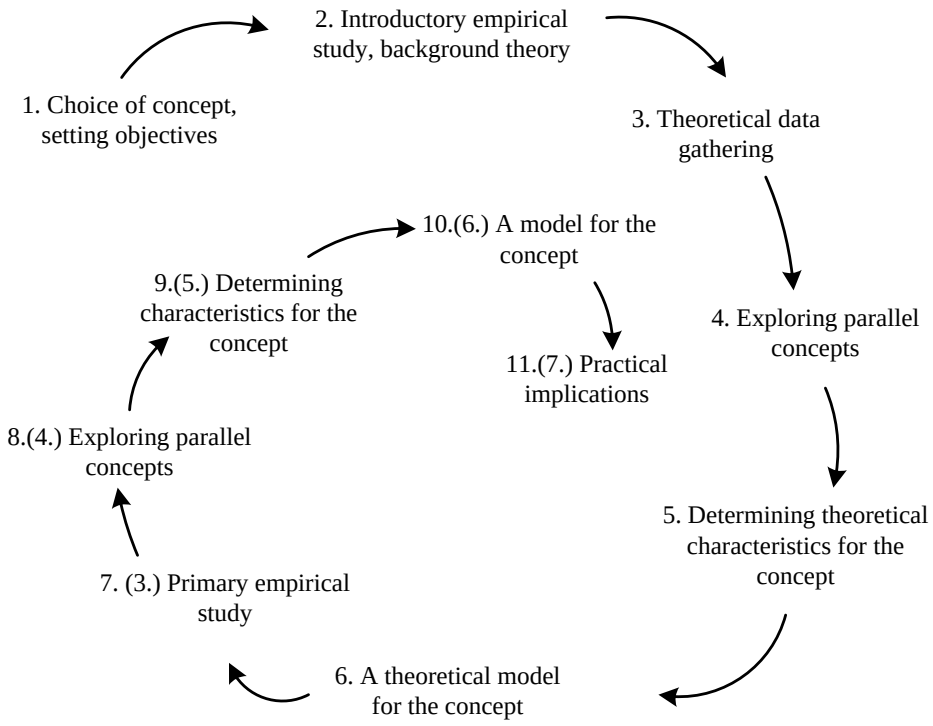

Figure 8: The research strategy and illustration of the conceptual analysis phases

In line with Figure 8's phase 2, the introductory empirical material was used for narrowing the research setting. The theoretical and empirical parts of the study were planned in this phase, but the plans were adjusted along the way. The use of qualitative methods in the empirical portion of the research was established early on, since it was

obvious that the explorative approach of this study would not suit quantitative methods well.

In the third phase in Figure 8, the theoretical material was gathered, and a systematic survey of literature on the concept of knowledge security was performed. The cyclical nature of the model is manifested in the dialogue between the theory and empirical material. Steps 3 to 6 in Figure 7 were repeated during the theoretical and empirical portions of the work, first in the theoretical and then in the empirical study. The author's initial intention was to go through all issues of 12 journals for a span of 10 years. The purpose of this systematic action was to find out what top journals say in the area of knowledge security. After a review of these journals, it was clear to the author that keyword searches over several databases would be a necessary complement for a review of this topic. If there was scientific discussion of the concept of knowledge security over the decade considered, the top journals in information systems science, knowledge management, and information security management were not the forum for it.

The systematic review of top journals (phase 3) was not, however, conducted in vain. The review provided the author with insight into what topics the top journals in the two fields are addressing and, thereby, about where the interest of the scientific community lies. It also aided in determination of keywords for the ensuing database searches. The development of the plan for the literature review followed the reasoning of Webster and Watson (2002), who emphasise that concentrating on only a select few journals easily casts aside discussion that is relevant. Reviewing only pieces in the top journals may be helpful when the aim is to publish in the same journals, but otherwise keyword searches of multiple databases are more likely to point one to the relevant sources.

In the fourth phase, parallel concepts and characteristics of knowledge security were found in the literature. This phase was merged with the literature review of the previous phase; the parallel concepts were recognised in the literature as the searches for discussion of knowledge security unfolded. In phase 5, the theoretical characteristics of the concept and parallel concepts were used for further definition of the characteristics of the concept. In phase 6, these were used in construction of a theoretical model for the concept and for a theoretical definition.

In the next phases, steps 3–6 in Figure 7 were repeated from an empirical perspective. The phase numbers in brackets in Figure 8 refer to the corresponding phase numbers in Figure 7 and highlight the cyclical progression between the various research steps. In phase 7, the primary empirical material used in this study was gathered in semi-structured interviews. The introductory empirical material acted as a trigger to what is interesting about knowledge security and in this way pointed the way for the data collection. All of the interviews in this study were recorded and transcribed. The recording freed the researcher from the task of taking detailed notes during the interviews and enabled genuine discussion between their participants. Since the

interviews were semi-structured, they left quite a bit of room for the interviewees to express their ideas about knowledge, knowledge security, and knowledge management. The exploring of parallel concepts (phase 8) was thus done at the same time as the gathering of interview data, and these concepts were analysed in tandem with the primary analysis of the empirical material. In this sense, phase 8 was performed simultaneously with phases 7 and 9.

In phase 9, the characteristics of the concept of knowledge security were sought from the empirical material, for construction of an empirical model for the concept. Analysing interview transcripts by hand is tedious, so the aid of technological tools was sought. The qualitative analysis tool ATLAS.ti was used for coding and analysis of the interviews. The tool was of great assistance in finding the characteristics of the concept from the interviews. Thematic classification of empirical material can work for both theory-building and 'testing' (Weber 1990, Hsieh & Shannon 2005). The empirical research method used is described in more detail in Chapter 5. The empirical analysis produced a set of characteristics or elements that are seen in companies as being related to knowledge security. These characteristics form the empirical model for the concept.

In phase 10, a model for the concept was constructed, via synthesis of the theoretical and empirical models. Accordingly, the model is a result of interplay between the theoretical and empirical material. The role of the background theories in the model is discussed in this step, and a definition of the concept (knowledge security) is formulated and parallel concepts analysed. In the final phase, the practical implications of the analysis and the concept that is constructed are discussed. In this study, the implications emerged largely from the interviews and the participants' insights. The practical implications are presented in this work more as discussion than as suggested actions; however, the discussion may inspire thinking and lead to changes in some companies.

1.4 The research process and structure of the study

The primary research objective in the thesis project has been to analyse the concept of knowledge security, with the objective met by answering the research questions presented in Section 1.1. The core outcome of the study is an analysis of the concept of knowledge security. The empirical material provides insight into the practical implications of that concept. The research process, which is the implementation of the research strategy, is illustrated in Figure 9.

The strategy in this research has been to make parallel and consecutive theoretical and empirical advances leading to a comprehensive conceptual analysis. The traditional research approach of first concentrating on theory, then moving on to empirical study would not have worked, since the interplay between the theory and practice was a very important factor in the analysis. The introductory empirical grounding helped to focus the theoretical study and triggered research questions for the systematic literature

review. The literature review, in turn, affected the research setting for the primary empirical study and guided the analysis of the empirical data. The theoretical examination of the parallel concepts has been affected also by the primary empirical material, so there has been dialogue of empiria and theory throughout the study.Research begins when the primary objective is set. The objective sets the direction for the research efforts. A typical doctoral study process takes several years and includes many moments of learning and comprehension. It is unsurprising, then, if the objective and the research questions change several times in the course of the process. The research design here showed flexibility for this pattern, which indeed was seen in the present study.

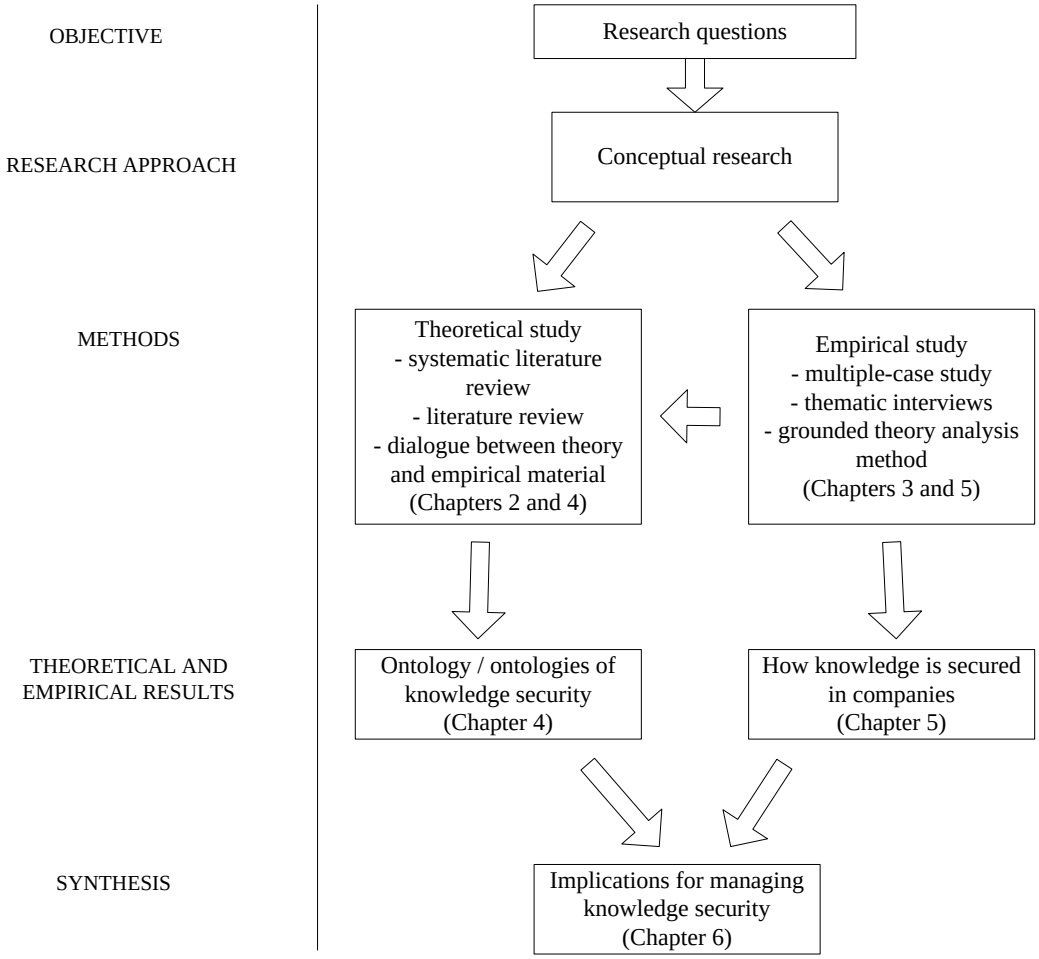

Figure 9: The research process

The research approach of this study is conceptual analysis as described above. The conceptual research approach, which lies in the middle ground between objective and subjective approaches to science, calls for both theoretical and empirical material to be gathered, so that both the idiographic and the nomothetic dimension are taken into account (see Figure 4, on p. 9). The idiographic dimension implies that one can understand the social world only by obtaining first-hand knowledge of the subject under investigation through getting close to it and gathering history and background information on it. The nomothetic approach, on the other hand, places emphasis on the

importance of basing research on a systematic protocol and technique. (Burrel & Morgan 1979) The middle ground chosen in this study entails systematic gathering of the theoretical material and a more flexible approach to empirical data.

The research process is aimed at formulating both a theoretical and an empirical contribution, which can then be synthesised for conclusions as to practical implications. The research tradition in the field of industrial management, a broad umbrella under which this study can be situated, emphasises practical implications. Since this study is not action research and concrete practical contributions cannot be shown, the theoretical contribution is also of vital importance in this study. Although some authors may regard conceptual analysis as purely theoretical (Puusa 2008), a concept is empty if it does not have a manifestation in practice. A concept has the dimensions both of a theoretical definition and of a practical phenomenon (Niiniluoto 1984) (see Figure 2, on p. 7). This is also why the contributions of this study are both theoretical and practical in nature.

In this chapter, the discussion of philosophical and research approach choices made in this study has provided insight into why and how the research has been carried out. Research in the making is chaotic and can even be highly fragmented, although the research approach models may appear simple. Aligning one's study with a specific philosophical approach or research paradigm helps the researcher to make and support the choices that arise in the course of the process. At the same time, the various models provide windows to what kinds of choices are possible and perhaps common in the relevant field of research. Discussion of methodology is discussion of how the research contributes to science.

In line with the steps of conceptual research, the roots and background theories of knowledge security are discussed in Chapter 2. The third chapter introduces the introductory empirical study, which motivated further conceptual analysis. The interplay between theoretical and empirical material began with the introductory study: it triggered questions for the literature review that is reported upon in Chapter 4. The concept of knowledge security and parallel concepts are examined in theoretical terms in the review, and a theoretical model of the concept is presented at the end of Chapter 4.

The interplay between theory and empiria continues with the theoretical model, establishing a basis for the primary empirical study. In Chapter 5, the implementation of the qualitative empirical research design is described and the findings are presented. Chapter 5 concludes with introduction of the empirically identified characteristics of the concept of knowledge security.

In Chapter 6, the theoretical and empirical work are brought together in a model constructed for the concept of knowledge security. Discussion of theoretical and empirical contributions is provided in Chapter 6, along with conclusions and implications for practice. At the end of the final chapter, the study is evaluated and avenues for further research are discussed.

2 Theoretical background

This chapter discusses the theories and concepts constituting much of the background for the study. The main fields of theory informing the work are knowledge management and information security management. The concept of knowledge is examined from different perspectives, to allow a good understanding of what the term ‘knowledge’ means in the context of this study.

The background theories are presented and analysed for building a foundation from which the actual conceptual analysis is performed. The outcome of this theoretical analysis is not a model that can be empirically tested. Instead, the outcome is a theoretical framework rooted in the main background fields and their combined analysis. In the conceptual analysis as depicted in Figure 7 (see p. 14), this chapter represents step 2. This means that the chapter introduces the background concepts that guide the further gathering of theoretical and empirical data. However, this chapter is also in one sense the first round in the cycle through steps 3 to 6 of the conceptual analysis process. In this work for the chapter, the theoretical basis for the concept of knowledge security was built, and this basis is also part of the conceptual analysis itself.

2.1 Knowledge

Depending on the user and the context, the term ‘knowledge’ can mean a variety of things. It can mean information stored and processed by various kinds of computer systems. It can also imply information stored in libraries in the form of books and journals. Or it can mean the knowledge of employees, either residing in their heads or stored on computers as documents on work processes etc. The differences and difficulties in definition of the term ‘knowledge’ are partly caused by the lack of a general expression in the English language. For example, in the field of information security, it is rare to specify what exactly is meant by the word ‘information’. Rather, the definition is implicitly assumed to be understood by all readers.

In this section of the work, the terms that are important for this study are presented and analysed. The term ‘knowledge’, as part of the concept under analysis, needs to be examined in detail before it can be defined. In this section, several definitions of the term are analysed, and a synthesis of them is developed for the purposes of this study.

2.1.1 Information summarisation

One approach to clearer definition of what is meant by the concept of knowledge involves looking at it from a hierarchical perspective. According to several authors (Thierauf 2001, Awad & Ghaziri 2004, Hislop 2005), there are anywhere from three to six levels of information summarisation. All of the authors cited above agree on the

three lowest levels; data, information, and knowledge. What is above knowledge in the hierarchy, however, is under debate. Thierauf (2001) presents a hierarchy of six levels of information: data, information, knowledge, intelligence, wisdom, and truth. In Figure 10, the levels are presented up to the level that is referred to as intelligence.

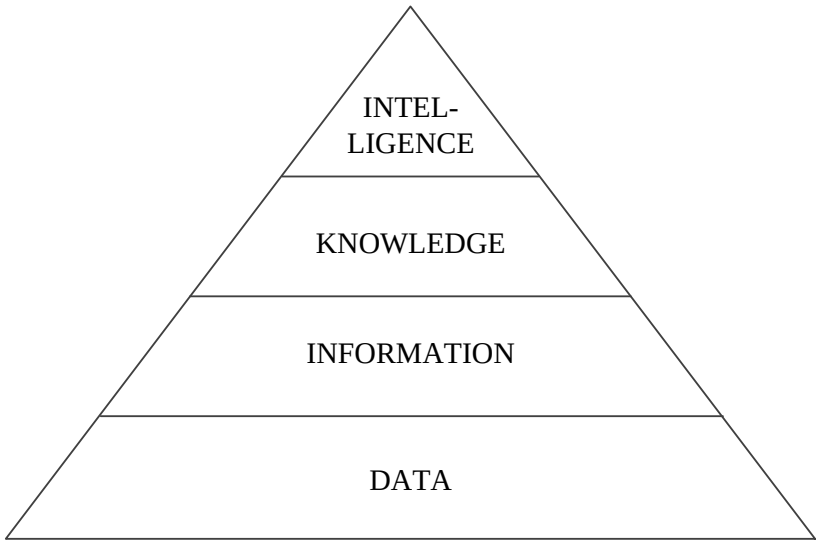

Figure 10: Levels of information summarisation

The lowest level in the hierarchy in Figure 10, data, represents unstructured facts and figures, the raw results of observation or measurement (Hislop 2005). Companies store data in large quantities, but said data must be automatically stored and processed, as the ability to prioritise and rank data decreases in direct proportion to the quantity of data being used (Thierauf 2001). This means that often the sheer volume of data renders processing it by any human impossible. The level of data is the lowest in the hierarchy, and, to be useful, data must be structured and placed in context. A typical example of data is individual numbers and figures stored in a database table. Without details contextualising the data recorded in the table, the data do not offer much value. The definition of data is subject to little debate among the various authors of relevant works.

The next level up in Figure 10, information, is structured data – data in a form that is useful for analysis (Thierauf 2001) and organised into a meaningful pattern (Hislop 2005). In other words: information is data organised in a certain form. Information is more qualitative than data (Awad & Ghaziri 2004). Information can also be described as data in context; for example, a database table becomes information when the rows and columns of the table are given names, as explanation thus is given to the data recorded. For instance, the rows might be dates and the columns years, and the data entries temperatures in degrees centigrade. Although information is dependent on context for its interpretation, once the context is established, the information is objective. This means that the figures are the same for all people reading the contents of a database, and everyone who can read the table agrees that the temperature in Tampere on 20 Dec. 2011 was 0 degrees Celsius, if that is what is recorded in the database.

The information hierarchy can be illustrated as a triangle with data forming the base on which knowledge and the other higher levels rest (Awad & Ghaziri 2004). This indicates a one-way process, with the higher levels being generated from the lower levels, as illustrated in Figure 10. However, the interrelationship is more complicated than that, and in many cases knowledge and intelligence are needed for generation of data and information (Hislop 2005).

According to Thierauf (2001, p. 8), knowledge is something obtained from experts on the basis of experience. A range of information must be integrated before one can perform analysis and make decisions. Thierauf states that if information is data about data, then knowledge is information about information. This rather cryptic statement means that knowledge is a structured collection of information. However, what is that element that provides information about information? According to Hislop (2005, p. 16), knowledge provides a means to analyse and understand data and information and serves as a grounding to guide meaningful action and thought. Nonaka and Takeuchi (1995, p. 58) add that it is context-specific and relational. These aspects make knowledge a mix of experience, values, contextual information, insight, and intuition that provides an environment and framework for evaluating and incorporating new experiences and information (Davenport & Prusak 1998). In the context of the database example above, one observer can conclude from a database showing temperature records that the days in July are warmer than the days in December in the northern hemisphere. An observer with knowledge of statistics can use the database to extract trends and possible changes in weather over the years. So the information about information that Thierauf (2001) writes about is mediated by experience. With experience, people are able to explain information, and this is what we call knowledge.

What comes above knowledge in the information hierarchy depends on the author. According to Thierauf (2001), there are three levels here: intelligence, wisdom, and truth. Other authors settle for intelligence or insight (e.g., Choo 2002, Awad & Ghaziri 2004), which is reasonable also in the case of this study since definition of wisdom and truth requires a great deal of philosophical discussion that still yet is not going to lead to conclusive agreement. Intelligence is seen as something higher than knowledge, more useful and more refined. It is also something that many authors link to decision-making (Drott 2001, Frishammar 2003). To be able to make their decisions, companies need interpreted and insightful knowledge about their situation. If one applies Thierauf's (2001) characterisations to this level of information summarisation, intelligence or insight is knowledge about knowledge: experience-based analysis of knowledge.

The summarisation levels serve as one way to understand the fact that we need large quantities of data and information in order to form knowledge and intelligence. However, without knowledge and experience, we cannot interpret data and information, or in some cases even create them. Clearly, therefore, the hierarchical model is not exhaustive. Neither does it fully explain what those higher levels consist of.

2.1.2 Dimensions of knowledge

According to Maier (2010), knowledge comprises all cognitive expectancies that an individual uses to interpret situations and to generate activities, behaviours, and solutions, no matter whether these expectancies are rational or used intentionally. This broad definition of knowledge reveals that there are dimensions to knowledge that can be examined more deeply, and that knowledge is tied to the cognition of the knower. There are numerous typologies of knowledge (Maier 2010, pp. 68–69) that categorise knowledge along dimensions such as tacit to explicit or individual to social knowledge.

The various categorisations of the term 'knowledge' have been developed to explain what characteristics the knowledge has and where it resides. The categorisation into tacit and explicit knowledge has been particularly subject to debate, surrounding whether these two categories are separate from each other and thus exclusive or, instead, involve two different dimensions of knowledge and therefore can exist simultaneously (McAdam et al. 2007, Assudani 2009, Oguz & Ayse 2011). In Table 1, different categorisations and dimensions of knowledge relevant for this study are compiled. The table is inspired by the work of Maier (2010) and similar collections, by other authors.

Table 1: Dimensions of knowledge, according to various authors

Dimensions	Authors
1. Tacit 2. Explicit	Polanyi (1968), Nonaka and Takeuchi (1995)
1. Individual 2. Collective	von Krogh (2009)
1. Individual 2. Social	Russell (1948)
1. Embrained 2. Embodied 3. Encultured 4. Embedded 5. Encoded	Blackler (1995)
1. Codified 2. Personalised	Hansen et al. (1999)
1. Information 2. Know-how	Kogut and Zander (1992)
1. Know-what 2. Know-how 3. Know-why 4. Care-why	Quinn et al. (1996)

Nonaka and Takeuchi (1995) brought the concepts of tacit and explicit knowledge introduced by Polanyi (1966 in Nonaka & Takeuchi 1995) into the larger discussion in the management field. By explicit knowledge they mean knowledge that is transmittable in formal, systematic language. It can be stored in systems and documented; i.e., it is codified knowledge. Codification renders it fairly easy to transfer, distribute, and control (Nonaka & Takeuchi 1995, p. 59). Codification makes explicit knowledge also independent of context, and impersonal (Hislop 2005, p. 19). Hansen et al. (1999) refer to these properties of codified knowledge with their own dimensions of codified and personalised knowledge. Codified knowledge is knowledge that is made independent of the knower, or detached from the person. Information in the dimensional system of Kogut and Zander (1992) is close to explicit and codified knowledge, and Blackler (1995) calls the same knowledge 'encoded knowledge'.

Russell (1948 in Maier 2010) and later von Krogh (2009) specify individual and social or collective dimensions to knowledge. These dimensions differ from the other classifications in Table 1 in that there is no dimension separating knowledge from the character of the knower. According to the above-mentioned authors, the knowledge is tied to either the individual or the social interaction of a collective of individuals. In addition to these two authors' work, all dimensions and categories presented in Table 1 emphasise that knowledge has one or more dimensions that are strictly tied to the individual who possesses the knowledge, the knower. Below, in Table 2, the definitions of dimensions linked to the knower are further examined. The dimensions of encultured, social, and collective knowledge are included in this group because they indicate a strong role of the individual as part of the social interaction or as a member of a collective.

Table 2: The features of dimensions of knowledge tied to individuals

Term	Features	Examples
Tacit	Knowledge of experience, highly personal and hard to formalise, tied to a certain situation. Embedded in feelings, intuition, and understandings (Nonaka & Takeuchi 1995).	'We can know more than we can tell' (Polanyi 1968 in Nonaka & Takeuchi 1995). We know how dough feels when it is right, how we maintain balance on a bicycle, and how a speaker knows how to gain the attention of an audience.
Individual	Being tied to the feelings and experience of the individual (Russell 1948). The individual being able to gain new knowledge through experience (von Krogh 2009).	Each individual has his or her own interpretation of words, and we can try to express this knowledge in language by using metaphors that convey feelings. I have the experience of working on a study, I know how I feel about it, but I can only describe this feeling to others. They cannot have the same knowledge.

Term	Features	Examples
Collective	Collective knowledge born of interaction between individuals (von Krogh 2009).	In problem-solving situations, each individual brings his or her own idea of how to solve the problem, and a solution can be found through collective combination of the ideas.
Social	'The community know[ing] both more and less than the individual'(Russell 1948 in Maier 2010). When knowledge is conveyed in words and interaction, it becomes social. However, there are differences in how the language is interpreted by individuals.	When employees of a company describe the functionality of a machine, they create social knowledge of the topic.
Embrained	Abstract knowledge that depends on conceptual skills and cognitive abilities (Blackler 1995).	This involves people's ability to link abstract theories together: University learning emphasises embrained knowledge.
Embodied	Action-oriented knowledge that is only partly explicit (Blackler 1995).	The way workers know how to operate a machine. A musician embodies the music played.
Encultured	Knowledge that is part of the process of achieving shared understandings (Blackler 1995).	This is seen in the way a group of workers use illustrative language surrounding their work.
Embedded	A link to social and institutional arrangements, residing in relationships between roles and routines (Blackler 1995).	The secretary knows about routine tasks, and the third-floor accountant has good relations with a certain customer.
Personalised	Knowledge as used to invent new solutions, with each person possessing unique knowledge and insights (Hansen et al. 1999).	A management consultant, understanding the differences between companies and their situations, is able to use this understanding when inventing suitable solutions for each company.
Know-how	A description of knowing how to do something, how to organise work (Kogut & Zander 1992). The ability to apply the rules of a discipline to complex real-world problems (Quinn et al. 1996).	Including the 'recipes' for carrying out work, this involves individual-level skills that are hard to transfer to others.
Know-why	Systems understanding and in-depth knowledge of the web of cause-and-effect relationships (Quinn et al. 1996).	The intuition of a manager in making decisions and comparing alternatives is a good example.

By tacit knowledge Nonaka and Takeuchi (1995) refer to knowledge embedded in people, which can be described as 'know-how', 'know-why', insight, understanding,

skill, etc. Since tacit knowledge is bound up with people, it is not easy to distribute and share widely, because its communication requires effort from both the person delivering the knowledge and the person receiving it. It is subjective, personal, and context-specific (Hislop 2005). Nonaka and Takeuchi (1995) describe a process model of sharing and creation of knowledge at a company, a model based on the continuous transformation of knowledge from tacit into explicit form and back. The key to success, according to these authors, is the ability of the company in question to harness tacit knowledge efficiently.

Tacit knowledge was initially described by Polanyi as a process of knowing, rather than as an object (Tsoukas 2003, McAdam et al. 2007). If one views tacit knowledge as a process in nature, it comes naturally to link the dimension of tacit knowledge with the dimensions of embodied knowledge, embedded knowledge, and encultured knowledge. All of these describe a process rather than an objectifiable phenomenon. 'Knowing' as a term leads one to think about knowledge as dynamic and useful: knowledge is manifested in the situations in which it is used.

Embedded knowledge is linked to roles and routines (Blackler 1995). Thus it is bound to the people who have learned the routines and is passed on as knowledge about tasks. In that sense, embedded knowledge may remain even if who handles the routines changes. Encultured knowledge is also linked to the interactions between people. It is manifested in how people communicate and work together, 'the way things are done and how people talk'. In this sense, encultured knowledge can be compared to 'organisational culture' (Schein 1984). The term 'encultured knowledge', however, describes a process and understanding of the culture, whereas 'organisational culture' refers to the phenomenon of that culture itself.

'Embrained knowledge' as a term refers to the ability of the knower to apply his or her knowledge and understand abstract theories. Embrained knowledge is linked to 'know-what' (Quinn et al. 1996), in that it refers to knowledge that applies theory through the experiences of the knower. Although embrained knowledge is strongly linked to theoretical knowledge, which can be considered expressible in explicit form, the aspect of embrained knowledge that is tied to the ability of the knower to apply that knowledge connects it to the knower – embrains it in the knower. This difference also explains why embrained knowledge is included in Table 2 and know-what is not. Embrained knowledge is similar in definition to 'know-why', the intuition of the decision-maker to apply the underlying theoretical knowledge to various situations.

Knowledge is tied to either individuals or a collective of individuals. According to von Krogh (2009), individual-level knowledge provides people with the capacity to reflect, think, plan, decide, act, and compass and solve problems in the workplace. At the collective level, knowledge allows for communication, co-ordinated reflection, thinking, planning, decisions, and action (von Krogh 2009). Both of these levels need to be accounted for when knowledge in companies is examined, and much knowledge

comes about via the transition from individual to collective and back. As von Krogh states in his paper, both perspectives need to be present, and they are indeed seen in a great deal of research. What von Krogh calls collective knowledge is quite similar to what Blackler (1995) terms encultured and embedded knowledge. However, Blackler (1995) does not place so much emphasis on the problem-solving purpose of encultured or embedded knowledge. While this is not stressed, the characteristics of embedded knowledge can be concluded to be important in problem-solving situations: the connection between roles and people's routines is what makes efficient problem-solving and reactions possible.

The concept of knowledge has been examined by many authors, and the list presented here is nowhere near exhaustive. However, it presents perhaps the most commonly used categorisations of knowledge dimensions. Different dimensions from various authors are also very close to each other, as is clear above. The role of a person, the knower, as a key element in knowledge is evident. Next, the results of this analysis of the dimensions of knowledge were utilised in devising the definition of knowledge used in this study.

2.1.3 Knowledge within the scope of this study

Knowledge and the higher levels in the information hierarchy (see Figure 10) are mostly tacit or embrained and embedded in nature. This means that knowledge is tied to people. In a strict interpretation of some of the above definitions, knowledge cannot exist without people. Information and data, on the other hand, are explicit in character. As to where exactly the boundary between tacit and explicit knowledge lies, it is hard to pinpoint. This is because knowledge can be seen as on a continuum whose one extreme involves something fully tacit (a person does not know that he or she knows something) and the other extreme something completely explicit (raw figures printed on paper).

In this study, knowledge is seen not as a general concept but as a part of a hierarchy. The focus here is on knowledge that is important for a company and that, in general, cannot be protected through common technical measures such as anti-virus protection, firewalls, and backup routines. Knowledge, according to the above definition, resides mostly in the heads of employees. It is based on their experiences, insights, skills, and interactions. It has characteristics of all dimensions listed in Table 2. Figure 11 illustrates the forms and routes of this knowledge, for better insight into the nature of the knowledge under examination.

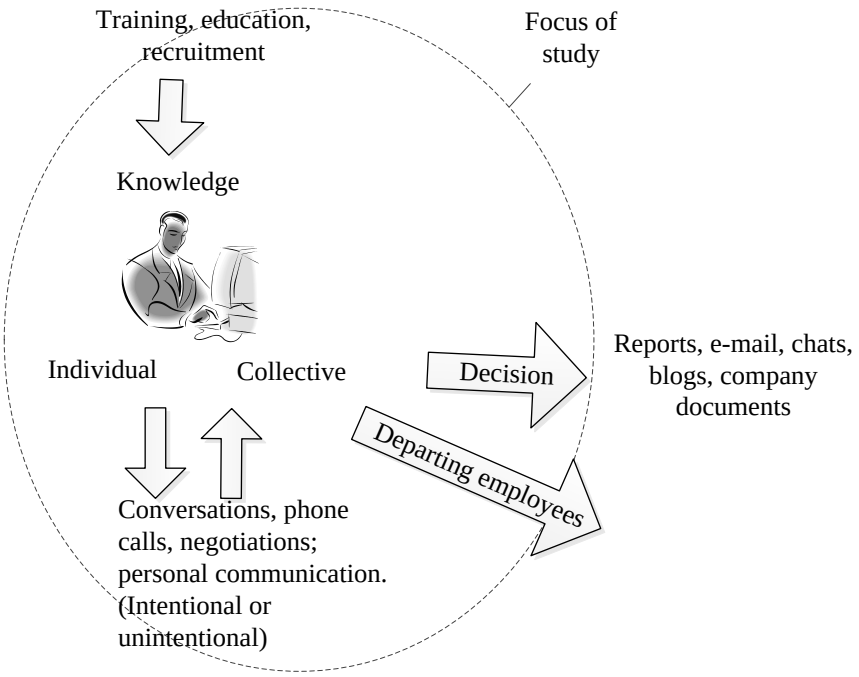

Figure 11: Knowledge within the scope of this study

Figure 11 illustrates the focus of this study: on individual and collective knowledge that resides within individuals working for a company. Even though documented knowledge in the form of e-mail messages, reports, and other materials does exist and these documents can be considered knowledge, they are largely beyond the scope of this work. Its scope covers the grounds for people's decision to create and deliver the documents – i.e., the importance of the knowledge and with whom it is shared.

As a synthesis of the various aspects of knowledge discussed above, the following characterisation can be derived: Knowledge is *embedded in people and their experiences. It is manifested in social interactions and in situations wherein people use their skills and experiences to solve problems and create new knowledge. Knowledge is embedded in people's tasks, roles, and routines, as much as embrained in their abstract understanding.* The business context adds the dimension of importance to this definition. Not all knowledge that is embedded in people is relevant from the point of view of a company. In the next section, the recognition of important knowledge is examined further.

2.2 Knowledge management

Nonaka (1991, p. 162) emphasises the importance of managing knowledge, in stating: 'Successful companies are those that consistently create new knowledge, disseminate it widely throughout the company and quickly embody it in new technologies and products.' Knowledge management is a discipline that examines approaches to, for example, the efficient creation and use of knowledge in companies. In this section of the dissertation, some approaches to knowledge management are examined more closely.

2.2.1 The general orientation of knowledge management

According to Schultze and Leidner (2002), knowledge management is generation, representation, storage, transfer, transformation, application, embedding, and protection of knowledge. Maier (2010, p. 57) defines knowledge management in a complex manner as a function responsible for selection, implementation, and evaluation of knowledge management strategies aimed at improved performance of the company. In summary, knowledge management can be defined as a collection of approaches to knowledge designed to improve a company's performance and competitive position.

The definitions presented above for knowledge management describe a collection of approaches to knowledge. These approaches can be analysed, for example, on the basis of their orientation toward human factors or technological solutions, as Maier (2010) has pointed out; see Figure 12.

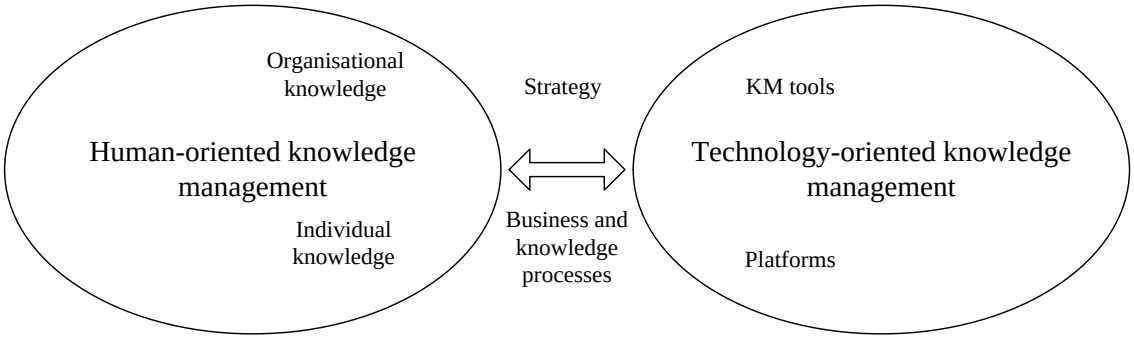

Figure 12: Orientations of knowledge management (drawn from Maier 2010, p. 53)

The technology- and human-oriented approach to knowledge management illustrated in Figure 12 are distinguished from each other by the kinds of solutions that are used for managing knowledge. Technology-oriented solutions rely on technology, information systems, to provide solutions for knowledge management initiatives, while the human-oriented approaches emphasise 'softer' managerial approaches. A crude general characterisation of these two orientations is that the technological orientation involves concentration on explicit knowledge while the human-oriented approach focuses on tacit knowledge.

Another way to approach knowledge management is to describe or distinguish among the factors in knowledge management, such as those presented in Figure 13, by Awad and Ghaziri (2004), whose factors include a human, or 'people', factor and a technology factor that are quite similar to the ones presented in Figure 12. Awad and Ghaziri add a third factor, though: processes – to emphasise that all processes of companies include knowledge and that the knowledge itself is quite often a result of a process.

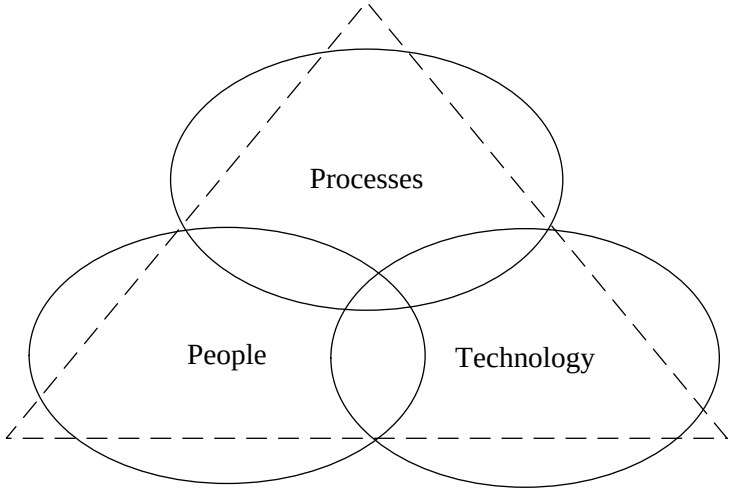

Figure 13: The basic factors of knowledge management (Awad & Ghaziri 2004)

The basic factors in knowledge management aid in recognising the locations of knowledge and in approaching solutions for managing knowledge. The people—technology—process model illustrated in Figure 13 emphasises the process dimension of knowledge management. In Figure 12, that element was depicted as falling between the human- and technology-oriented approaches to knowledge; however, the process dimension deserves much more attention than that, because most approaches to knowledge management can be described as, and usually considered to be, processes. The factors illustrated in Figure 13 form a very general approach to knowledge management and can best be utilised after the approaches to knowledge have been addressed in more detail.

In the sections that follow, a selection of these approaches is presented, to show the foundations on which the conceptual analysis of knowledge security are built. In the previous section, knowledge was defined as embedded in people and their experiences, as much as manifested in interactions and problem-solving. Further on, the focus of this study is defined as being on people's interactions and the decisions people make about what knowledge to codify and share. The study is also limited to knowledge that is important to companies. Accordingly, the aspects of knowledge management that are interesting for purposes of this study are knowledge recognition, knowledge sharing and transfer, knowledge creation, and codification and personalisation. In the next subsection of the work, the recognition of important knowledge is discussed, with a review of how different authors have discussed knowledge and knowledge management. The historical aspect of this section gives the reader a look at what knowledge companies have considered important in the past few decades.

Once knowledge is either implicitly or explicitly recognised as important, a strategy for its management can be considered. Therefore, the codification and personalisation strategies and their implications are discussed as key representatives of knowledge

management strategies. Then, theories of knowledge creation and of knowledge sharing and transfer are discussed, for a more in-depth view of what a company's knowledge processes can look like and what kinds of problems may be connected with them.

2.2.2 Knowledge recognition

For something to be managed, it first needs to be appropriately recognised. The previous section defined the concept of knowledge for the purposes of this study. How companies can recognise what kind of knowledge is important is one consideration in – and a prerequisite for – managing and harnessing that knowledge. However, the recognition angle is found surprisingly rarely in mainstream knowledge management literature.

In economic theory, the competitive position of a company is traditionally seen as an aggregate of various factors, such as market share, performance, and the imitability of the products (Lippman & Rumelt 1982, Prahalad & Hamel 1990, Barney 1991, Johnson & Scholes 2002). Lippman and Rumelt (1982) describe a factor called uncertain imitability that provides companies with competitive leverage. However, they do not specify what exactly 'uncertain imitability' is. They only state that it is a factor that differentiates companies from one another. The idea of imitability of products leads the reader to think about the way in which a company utilises the know-how and knowledge of an employee. In this light, uncertain imitability can be understood to refer to what kinds of knowledge assets companies have and how they use these as a differentiating factor, but Lippman and Rumelt (1982) do not provide verification of such an analysis.

In a groundbreaking article on the resource-based view of the firm, Wernerfelt (1984) argues that the set of resources a company possesses has a key role in its success. The way a company manages to exploit and develop these resources determines the company's competitive position. This can be viewed as somewhat of an expansion of the uncertain imitability of Lippman and Rumelt (1982). A company that succeeds in exploiting and developing its resources in a way that is difficult for competitors to imitate gains competitive advantage. Wernerfelt (1984) concludes his article with the remark that identifying individual resources is difficult. What characterises the resources that provide competitive advantage is that they either neutralise threats or exploit opportunities (Barney 1991). In other words, if a company has knowledge that enables it to counter competition (act against a threat) or increase the distance from the competition (exploit an opportunity), that knowledge is a resource. The resource-based view of the firm is a step further toward recognising knowledge as an important resource and asset to companies. Technology-related knowledge is cited as an example of a resource. However, knowledge is not considered any different from other resources; the resource-based perspective treats all resources as more or less equal.

In the ’90s, knowledge was acknowledged as ‘the one source of lasting competitive advantage’ (Nonaka 1991). The knowledge-based view of the firm (Grant 1996) recognises knowledge as a key resource that differs greatly from other resources available to companies. In that sense, it complements the resource-based view and goes further into what Wernerfelt stated was difficult to identify. However, Grant (1996) too states that knowledge is a concept that is hard to define, and thus difficult to identify. According to Grant (1996), companies’ success depends on their ability to combine and integrate knowledge, rather than just transfer it from one unit to another. This model seems to take for granted that the company has recognised which knowledge assets it needs to integrate in order to create value. Spender (1996) considers this ability from another angle and emphasises the firm’s capability of utilising collective knowledge. With the term ‘collective knowledge’, he refers to knowledge that exists in social connections – i.e., that is embedded in the processes of a company. Also, Kogut and Zander (1992) write about collective knowledge as the code of conduct within work groups. This knowledge is not always consciously recognised, yet it is important for the running and innovation of a company.

While Grant (1996) talks about integrating and combining knowledge, Spender (1996) argues that knowledge is constantly being merged and formed. Companies only have to find out ‘what it is about firms that enables collective learning to take place and collective knowledge to be retained and applied better than other institutional arrangements’ (Spender 1996, p. 52). Spender argues that a company is a dynamic entity and that knowledge especially is a resource that provides value when it is used. It is not a resource comparable to traditional physical and monetary resources; when used, the latter are no longer available. When knowledge is used, it is not consumed, and, furthermore, new knowledge can be generated through the use of knowledge. However, Spender (1996) does not analyse the recognition of knowledge further. He merely states that knowledge processes must be identified if one is to determine their value for the company and thus identifies a step toward recognition.

Another step toward recognising important knowledge is to discover the locations of this knowledge and the means of its transfer between locations. Argote and Ingram (2000) describe three locations, which they call reservoirs, in which knowledge resides: members, tools, and tasks. These three locations also form a collection of networks when combined. In the reservoir model, ‘members’ refers to the people working at a company; tools are the technological tools and information systems that companies use; and ‘tasks’ refers to the goals, intentions, and purposes of the company. (Argote & Ingram 2000) The reservoir model acknowledges that knowledge is embedded in people and their interactions, and that knowledge transfer is more difficult when the members, or people, are involved as one component of the knowledge that needs to be transferred. The combination of reservoir types can be seen as referring to what Grant (1996) has described as the combination and integration referred to above. Since the scope of this study encompasses embrained knowledge, the knowledge reservoirs of interest are the members, along with the reservoir networks that involve the members: member–member,

member–tools, member–tasks, and member–tools–tasks networks. Although the reservoir model was created from the knowledge transfer angle, it is useful also for approaching the matter from the standpoint of knowledge recognition.

There are many factors that affect the result of knowledge transfer efforts, among them the tacitness of the knowledge, the difficulty associated with the knowledge, and that knowledge's importance (Kang et al. 2010). The last of these factors listed by Kang and colleagues is of interest when one is speaking about knowledge recognition. They define important knowledge as knowledge that is strategically important. In other words, one way to recognise knowledge that is important to a company is to consider what knowledge is needed in strategic decision-making. In the traditional knowledge management literature, there seems to be a focus on where the knowledge lies and how it must be handled and transferred. This 'knowledge management point of view' is important in its own right but is difficult to operationalise, since there is no immediate connection to daily operations. Therefore, this point of view needs to be complemented with viewpoints from other fields of management, such as strategic management, marketing, and market and competitive intelligence. Widening the scope allows discussion of what the knowledge is about and of how we can know which knowledge is important or valuable.

Strategic management deals with strategic decisions in companies. Strategy is 'the direction and scope of a company over the long term, which achieves advantage for the company through its configuration of resources within a changing environment and to fulfill stakeholder expectations' (Johnson & Scholes 2002). Therefore, strategic decisions are decisions that have an impact on the future of the company. Also, they often involve an aspect of change (Johnson & Scholes 2002). One key to making effective strategic decisions is to follow a structured decision-making process and use well-analysed information, in sufficient quantities, as grounds for the decision (Dean & Sharfman 1996). However, although the decision-making process is important for success, it does not necessarily explain it fully. Knowledge and the experience of the decision-maker form another key factor for success (Brockmann & Anthony 2002). The ability to analyse the information and filter for what is relevant – i.e., the intuition of the person making the decisions – is important. It would be a tempting solution to say that important knowledge is only in the heads of decision-makers, that only the decision-makers know what knowledge is important, and that this recognition cannot be articulated.

Strategy literature emphasises the decision-making process and the importance of making informed decisions (Johnson & Scholes 2002). What kind of knowledge is needed for strategic decisions can be used as one key to recognising important knowledge. Market intelligence and competitive intelligence are activities or processes aimed at providing decision-makers with the best possible information as a foundation for their decisions (Hedin et al. 2011). The strategy literature quite often considers the most important topic related to information (or knowledge) to be competition (Lippman

& Rumelt 1982, Prahalad & Hamel 1990, Barney 1991, Wernerfelt 1984, Dean & Sharfman 1996). How to recognise the sources and the knowledge lying also inside the company is a challenge, since traditionally the focus of market and competitive intelligence activities has been on gathering knowledge from sources outside the company. Many times, however, a good amount of knowledge is to be found from the employees of the company (Hedin et al. 2011, Vuori & Okkonen 2012).

Not all knowledge is equally valuable or equally easily utilised. Strategic knowledge is oftentimes gathered from bits and pieces of information that together form a big picture on which one can base decisions. The ability to build this big picture, the embrained knowledge of managers, is one very important part of a company's knowledge. Recognising the bits and pieces of knowledge that are needed to build the picture is a challenging task – which is why knowledge recognition is needed. As has been pointed out above, it would be unwise to claim that only the decision-makers possess important knowledge. Middle-level employees or, for example, the maintenance staff of companies may have important insights about the needs of customers, future products of competitors, or customers' attitudes toward the products.

Marketing is another field that emphasises knowledge recognition. Marketing strategies need to be based on a broad picture of who the customers are, what they need, and what kinds of customers the company wants to attract (Kotler 2000). Providing customers with superior value is seen in the marketing literature as a key success factor (Payne & Holt 1999, Ling-Yee 2011). To know what is valuable to a customer, the company needs to know the customers and their needs well. This makes knowledge about the customers important.

The knowledge about customers and the market in general may lie in many places, and not all of those places are within the company (Hedin et al. 2011). Business partners and subcontractors may have a lot of insightful knowledge about the end customers of a company. This knowledge needs to be recognised and then shared with the parties that need it. Most companies are themselves customers, so they can provide important pieces of knowledge to their suppliers. Recognition of this knowledge may aid in both acquiring it for use in the company and trying to retain it at the company when needed. The various perspectives on recognising knowledge are summed up in Figure 14.

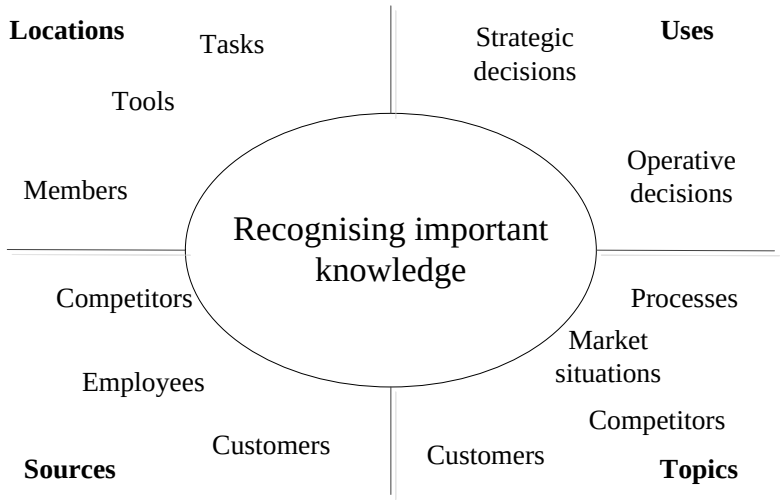

Figure 14: Perspectives on knowledge recognition

As Figure 14 illustrates, the location, sources, topics, and uses of important knowledge are angles from which one can consider recognition of that knowledge. From the discussion of knowledge recognition, one obvious fact emerges: there is a great amount of important knowledge. As the above discussion brings out, the most important knowledge is related to strategic decision-making and the competitive position of the company concerned. One part of knowledge of competitive position is to know what the customers want. The recipes for competitive advantage from these various angles seem to be quite similar, no matter the stream of the approach to knowledge: Utilise well the knowledge that you have, and you will win in competition. Regardless of the focus on strategic level in the streams of literature introduced, there is much important knowledge also at the operational level in companies. This knowledge is used in decisions at that level all the time. Hence, the above characterisation of important knowledge can be performed without the term 'strategic': the knowledge most important for a company is related to decision-making and the company's competitive position.

2.2.3 Personalisation and codification strategies

When companies have recognised which knowledge is important for their operations, a strategy for managing that knowledge needs to be chosen. The focus of the present study is on how employees treat the knowledge that is important for companies. The knowledge management strategy of codification or personalisation is one driver for what kinds of decisions people make when they share and document their knowledge.

According to Hansen et al. (1999), there are two distinct strategies to managing knowledge in a company. One is to approach knowledge through codification, and the other approaches knowledge through personalisation. Both strategies are aimed at efficient use of knowledge within the company. The difference between these strategies is in the way knowledge is perceived: as a codifiable, potentially multi-use asset or a

personal attribute. The codification strategy is intended to put all knowledge to efficient use by codifying it as much as possible, with the codification done via documentation of every solution created in the company, in knowledge bases. Problem-solving in such a company begins with searching for existing solutions related to the problem (Hansen et al. 1999). Codification involves the assumptions that important knowledge is codifiable and that it can be utilised in different contexts through its application by different users. In a company applying a strategy of codification, employees may be rewarded, for example, on the basis of the amount of knowledge they provide for the knowledge bases. A core aim is to capture as much employee knowledge as possible for the databases.

Although the codification strategy is intended to benefit a company by creating vast amounts of documented knowledge, it does not always work as intended. Codification may lead to overload, if employees are rewarded solely on the basis of the amount of knowledge they document. There is a danger of the knowledge bases being filled with irrelevant codified knowledge or multiple, redundant solutions. The codification strategy may backfire also on account of employees relying on the codified knowledge instead of trying to create solutions themselves (Chua 2009). In consequence, the company may lose potential creative future solutions, if people stop striving for them.

In contrast, at a company that applies the personalisation strategy, knowledge is perceived as personal and non-codifiable. Instead of investing in databases and time for documentation, these companies strive to enhance communication between employees and have master–apprentice and mentorship systems in place to ensure that important knowledge is passed from person to person (Hansen et al. 1999). Knowledge is seen as context-specific, and such companies emphasise personal ability to create solutions rather than apply existing solutions. In other words, companies that choose a personalisation-based strategy stress that knowledge cannot be separated from the knower, as seen in Table 2's depiction of the dimensions to knowledge (on p. 24).

Hansen and colleagues (1999) consider these two strategies to be alternatives: a company needs to choose between them, using the other of the strategies in only a supportive role. They provide empirical evidence that knowledge management initiatives must be based on either codification or personalisation. If a company tries to follow both strategies with equal emphasis, the initiative is going to fail. Scheepers et al. (2004) refine this theory by adding that an emphasis on one or the other needs to be chosen in the initial stages, but as the knowledge management programme in a company grows mature, codification and personalisation efforts tend to balance each other. A company that emphasises face-to-face communication needs to support it with well-functioning systems for finding the right people. Also, it is inefficient to have people only sharing their experiences with each other when they should be able to concentrate on their new assignments (Chai & Nebus 2012). This is why codification is needed in companies focusing on personalisation: to avoid inefficiency. Correspondingly, companies that have chosen codification still need personalisation, to help transfer

knowledge that is not easily codified; codification needs to be supported by opportunities to interact with the people who created the documents (Hansen et al. 1999, Hansen 1999). According to Chai and Nebus (2012), the strategies tend toward balance over time because companies must work efficiently, and concentrating on one strategy at the other's expense might lead to inefficient solutions and undesired redundancy.

2.2.4 The process of knowledge creation

Nonaka and Takeuchi (1995) proposed a process model of creating new knowledge in a company that is based on the continuous conversion of knowledge from tacit to explicit form and back. The model is called SECI, for its four constituent phases. The key to success, according to the authors, is the ability of a company to harness tacit knowledge efficiently in the four phases of the process: socialisation, externalisation, combination, and internalisation. In the socialisation phase, tacit knowledge is shared among colleagues when they are working together and observing others. In externalisation, the tacit knowledge is explicated through conceptualisations and models, as in documentation of a work process. In combination, the company's explicit knowledge is compiled and enhanced – e.g., transformed into reports on various work processes distributed to managers. In the internalisation phase, the explicit knowledge becomes tacit again when people implement new work processes (Nonaka & Takeuchi 1995). Figure 15 illustrates the SECI model.

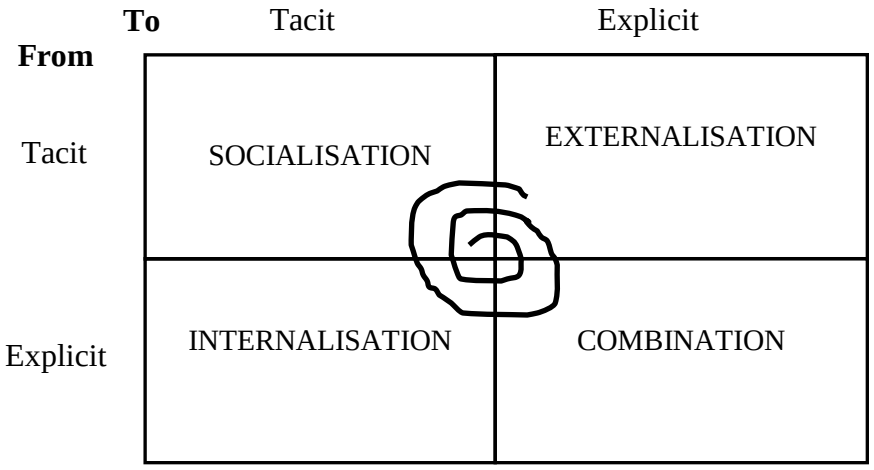

Figure 15: The SECI model (adapted from Nonaka & Takeuchi 1995)

The continuous interplay between the tacit and explicit slowly but steadily increases the company's knowledge. This process requires trust among employees, to enable socialisation, along with enough opportunities and time for sharing knowledge through socialisation and externalisation. The more knowledge is shared, the more new knowledge is created. (Nonaka & Takeuchi 1995) The spiral at the centre of Figure 15

denotes the cyclical nature of the SECI model and the idea that the amount of knowledge created grows with each cycle.

Application of the knowledge creation model can be seen as one way to implement both personalisation and codification strategies. If a company places great emphasis on the socialisation phase of the SECI model, it likely is following a personalisation strategy for managing its knowledge (Choi & Lee 2002). If, instead, the company emphasises codification, more active effort is being devoted to externalisation and combination. The SECI model nicely illustrates that both codification and personalisation are needed for new knowledge creation and that the choice of strategy only points to which phases are emphasised more than the others. Since, as noted above, the personalisation and codification strategies tend to become balanced over time, one can conclude that the emphases on different sets of SECI phases tend to even out.

Choo (1996) presents a model for a knowing organisation that complements the SECI model. This model of recognising and creating knowledge and basing organisational actions on it is presented in Figure 16. Whilst Choo's model uses the terms 'information' and 'knowledge' together in a manner that is not consistent with the definition of knowledge used in this study, the model is presented here with its original terms.

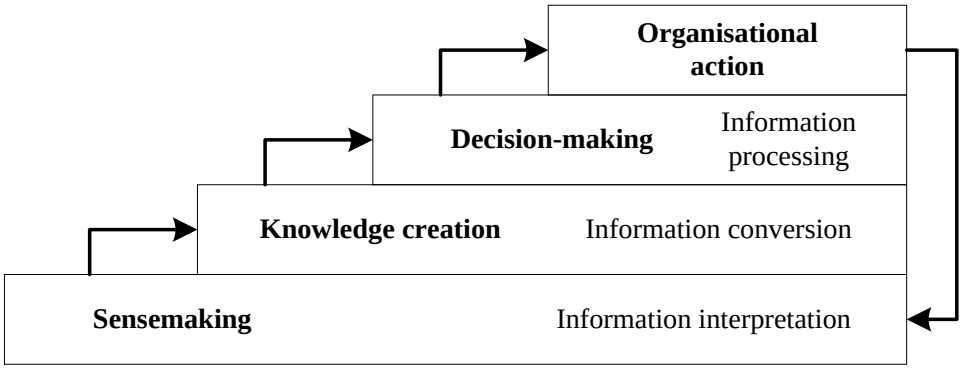

Figure 16: The Knowing Organization model (modified from Choo 1996)

In the model in Figure 16, the first step before knowledge's creation is one that many companies fail to take: sensemaking. This refers to companies' need to strive actively to figure out what kind of information is available to them, what the situation surrounding the company is, and what it means from the company's point of view. When a company has a good sense of what is going on around it, it can – for example, by building scenarios – create new knowledge that can be used in decisions on a plan for action. In the knowledge creation step in Choo's model, information about the prevailing situation is converted into knowledge about choices the company may have to make and about the consequences of these choices. In the next step, decision-making follows thorough analysis of the choices: information created in the previous phases is used for making informed decisions about actions the company should take. According to Choo (1996), when a company's actions follow this model, they are based on a shared and valid

understanding of the company's environments and needs, complemented by the members' knowledge and skills.

As is illustrated in Figure 16, the actions of the company lead to another cycle through sensemaking, knowledge creation, decision, and actions. According to Nonaka and Takeuchi (1995), a knowledge-creating company is one that can compete in the dynamic environment that companies face today. Choo takes this a step further and claims that, in addition to knowledge creation, there needs to be good interpretation of what the company is facing. In the sensemaking phase, a lot of knowledge valuation takes place. The people who attempt to make sense of the company's environment make decisions on which of the knowledge and information they have is important and which is not. In other words, they need to recognise important knowledge. The grounds for this recognition have been discussed to some extent in Subsection 2.2.1 of this work.

2.2.5 Knowledge sharing and transfer

Knowledge management is aimed at efficient sharing and free flow of knowledge within a company such that the company can maximise the benefits of the knowledge to it. Common sense tells us that if knowledge flows freely within a company, the right kind of knowledge is bound to reach the right people. However, structure to the sharing process is needed if one is to avoid irrelevant knowledge being shared or knowledge being shared with the wrong people, since this takes time and resources while yielding no benefits.

Studies have shown that knowledge sharing does not come about merely upon encouragement of communication with other people. For the knowledge sharing to be beneficial to all, there must be adequate co-ordination and trust among people but also not too many contacts between people (Willem et al. 2006). To be motivated to share knowledge, people also must feel that they get something of equal value in return (Barachini 2009). In some cases, knowledge is fairly easy to codify and hence share. In other cases, sharing is harder, because the knowledge is complex and thus difficult to codify adequately; here, sharing needs to occur on a more personal level. (Hansen 1999)

Knowledge transfer is an interesting topic in the knowledge management context since transferring knowledge from one unit to another requires the company's active effort. 'Transfer' refers to a conscious activity conducted on purpose (Argote & Ingram 2000, Kang et al. 2010). The goal of knowledge transfer is simple: to exploit knowledge accumulated in one unit or company for the benefit of other units or companies (Argote & Ingram 2000). However, knowledge transfer is not simple, even when the knowledge is in explicit form and thus readily accessible to the receiver (Hansen 1999). The terms 'knowledge sharing' and 'knowledge transfer' seem similar; the difference is in their end result. Transferred knowledge is knowledge that is actively shared and used by the receiver. This implies that knowledge sharing is a prerequisite for transfer.

Ipe (2003) describes knowledge sharing as an activity that makes knowledge available to other individuals. In this view, the sharing process requires conscious action on the part of the individual who possesses the knowledge at the outset. For the sharing process to be voluntary, the recipient of the knowledge must be considered worthy of joint possession of the knowledge. According to Ipe (2003), the main barrier to effective management from the knowledge management perspective is lack of knowledge sharing. To conquer this barrier, literature on knowledge management has emphasised enabling and encouraging knowledge sharing and building of trust among a company's employees (e.g., Nonaka et al. 2000, Chauvel & Despres 2002, Endres et al. 2007, Holste & Fields 2010, Swart & Harvey 2011). Ipe identifies four factors that affect knowledge sharing in companies. Illustrated in Figure 17, these are the nature of the knowledge, motivation to share, opportunities to share knowledge, and the culture of the work environment.

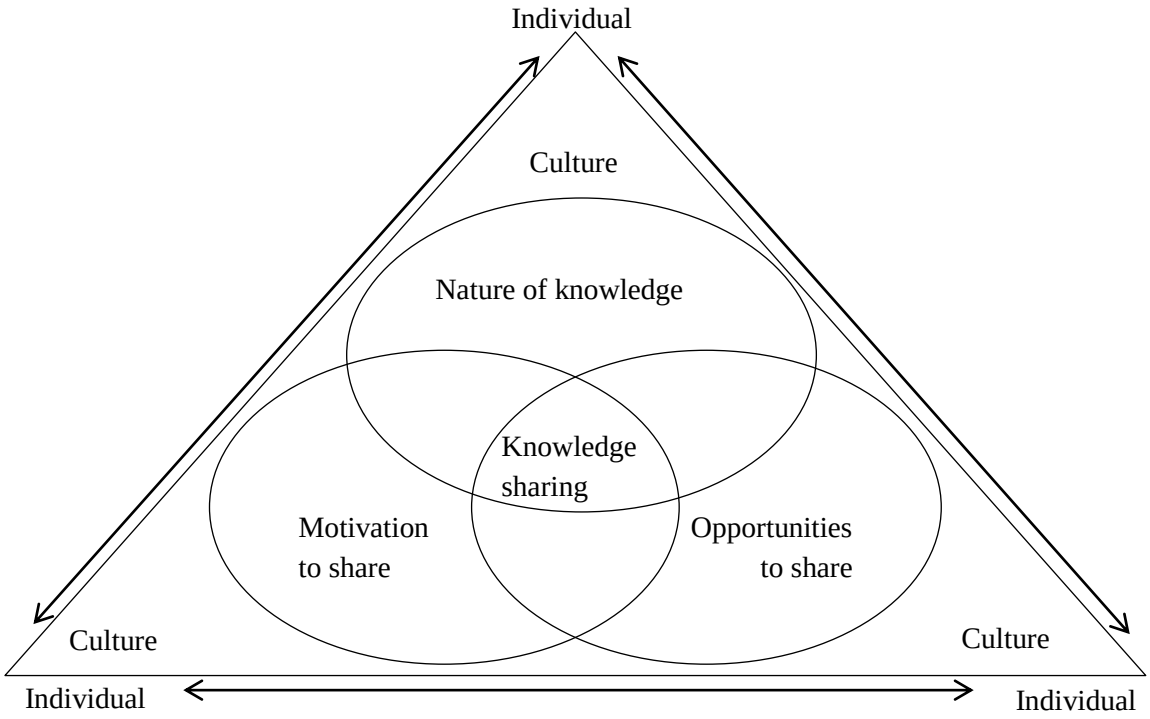

Figure 17: A framework for knowledge sharing (Ipe 2003)

The idea of the knowledge sharing framework presented by Ipe (2003) is that motivation and opportunities to share knowledge must be present. In addition, the nature of the knowledge needs to be such that sharing it is possible and the value of the knowledge is seen to increase through the sharing. When all three elements overlap, knowledge sharing can take place. Figure 17 illustrates that all of these elements co-exist within the organisational culture. Culture can support or hinder the knowledge sharing, and thus either promote sharing of knowledge between individuals or hinder it. This framework can be complemented with the term 'trust'. Trust among co-workers can be seen as one driver for motivation to share knowledge: if there is no trust between people, they are not willing to share knowledge with each other (Holste & Fields 2010). Opportunities to

share knowledge are created by, for example, the environment in which people work. How well a context provides opportunities for knowledge sharing is dependent in part on the environment (Nonaka et al. 2000). When all of the elements depicted in Figure 17 come together in the right way, knowledge sharing is promoted in the company.

Ipe (2003) argues that knowledge sharing occurs within a company no matter what the circumstances. However, how much and what knowledge is shared can vary greatly. When companies want to increase the value gained from sharing of knowledge, the framework for sharing comes into the picture. The framework can also be of assistance in knowledge creation and, in this case, used in combination with the SECI model illustrated in Figure 15. Along with the idea of a context for knowledge creation, 'Ba' (Nonaka et al. 2000), this knowledge sharing framework can complement the SECI model. It brings the organisational culture into the discussion of what affects knowledge sharing, and it also considers, for example, people's motivation to share knowledge. The SECI model (Nonaka & Takeuchi 1995) assumes that shared experiences generate socialisation. Ipe (2003) adds to this that people need to be willing to share and use the shared knowledge. These statements underscore that a company first must have in place a culture that supports knowledge sharing and active use of knowledge that has been shared: knowledge transfer. Cultural factors, the shared assumptions about how people at the company work together, greatly affect willingness to share knowledge, whether through face-to-face discussions and demonstrations or by knowledge codification.

2.3 Information security management

This section examines information security management as a key field whose theory provides underpinnings for the concept of knowledge security. Much of the terminology connected with knowledge security comes from information security management, so the meaning of the terms and the ideas behind those terms need to be presented.

2.3.1 Security

Before one delves more deeply into the perspectives offered by the information security management literature, it is worth analysing the content of the term 'security'. While the word is sometimes used as a synonym for safety, the two words have somewhat different dictionary definitions.

Security:

- The state of being free from danger or threat (*The American Heritage Dictionary of the English Language* 2009)
- The safety of a state or organisation against criminal activity such as terrorism, theft, or espionage (*Collins English Dictionary* 2006)

- Procedures followed or measures taken to ensure the security of a state or organisation (*Collins English Dictionary* 2006)
- The state of feeling safe, stable, and free from fear or anxiety (*Collins English Dictionary* 2006)

Safety:

- The quality of being safe
- Freedom from danger or risk of injury
- A contrivance or device designed to prevent injury

(*Collins English Dictionary* 2006)

From these definitions, we can draw the distinction that the term 'safety' encompasses both the idea of an object being protected from threats and the concept of that object not causing threats. The word is also strongly connected with physical damage or injuries. The term 'security' features only the perspective of an object being protected from threats, which may be physical or non-physical. For this study, the main concern is how to protect the knowledge residing within a company from threats, which justifies use of the term 'security'.

In the field of computing, the term 'security' has a close association with information:

Security:

- Prevention of or protection against

  a) access to information by unauthorised recipients or
  b) intentional but unauthorised destruction or alteration of that information

- Guarding against both unintentional and deliberate attempts to access sensitive information, in various combinations, in line with the circumstances (the concepts of security, integrity, and privacy are interlinked)

(Daintith & Wright 2012)

In the world of computing, safety, on the other hand, is linked more to the actions of products, especially software:

Safety:

- Freedom from risk
- A term also used in the context of 'safety level', in relation to quantitative measurement of the level of safety
- A concept used in the sense of a safe system as one that can never do anything bad

(Daintith & Wright 2012)

Another difference between the two terms has to do with the agent that is acting. Security can be seen in these definitions as something wherein the company itself is an active participant and contributor. With the term ‘safety’, the agent doing the protection is left more ambiguous, because the word refers to quality rather than to activity.

2.3.2 Information security

The previous section showed security to be closely connected with the term ‘integrity’. However, there is more to the term ‘information security’ than integrity alone. Information security is often defined in relation to three critical characteristics for information: confidentiality, integrity, and availability (Whitman & Mattord 2003, Peltier et al. 2005). These characteristics are illustrated in Figure 18.

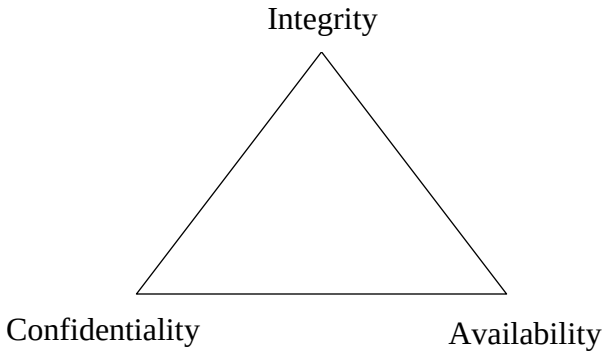

Figure 18: The ‘CIA’ triad of information security

Figure 18 presents these three characteristics in the order of their abbreviation ‘CIA’. The triangular shape adopted in the illustration is intended to highlight the independence of each; they are not necessarily dependent on each other or on the order in which the management prioritise them. Though the abbreviation is fairly easy to remember, it does not necessarily represent the only, or the correct, logical order for the characteristics.

Peltier et al. (2005) present integrity as the characteristic on which the other characteristics depend. Integrity refers to the accuracy and completeness of the information in all phases of its life cycle. This means that actions to guarantee integrity are aimed at the accurate (uncorrupted etc.) storage and processing of information. Confidentiality is presented as the element to be handled second. It refers to information being accessible to only those who are authorised to have it. Accordingly, actions aimed at guaranteed confidentiality concentrate on identifying who uses the information and on gathering information on who should be granted access to specific information. The final characteristic to ensure, availability, is defined as the information being available to those who need it, whenever it is required. This entails taking measures, which depend on the requirements, to guarantee uninterrupted access to information through,

for instance, redundant connections (Whitman & Mattord 2003, ISO/IEC 2005, Peltier et al. 2005).

This general presentation of the characteristics for information shows several angles on what kinds of characteristics information may have and on how they may be guaranteed. In this presentation, ensuring integrity comes first, since if the information is corrupted or lost altogether, there is no use in considering its availability. Furthermore, if it is not available to anyone, there is no need to limit access to it or otherwise address confidentiality. Although confidentiality might be the first of the characteristics to come to a reader's mind, it is the last thing to be considered when one is managing information security. Of course, this does not mean that it is the least important.

In addition to addressing the characteristics for secure information, information security includes a process that implements security measures in the areas of various components of security (Peltier et al. 2005). The components of information security that Peltier et al. (2005) list consist of areas of implementation to which the information security measures are to be applied. The number and names of the components vary with the author (Whitman & Mattord 2003, Tipton & Krause 2004, Peltier et al. 2005). In this study, a division into nine components is used. This classification is used in, for example, the VAHTI instructions created for Finnish public organisations by the Ministry of Finance (VAHTI 2009). Even though the VAHTI instructions were prepared for public organisations, most of the issues they cover are relevant also from the standpoint of companies, and, when comparing international literature, the author of the present work finds their breakdown of components of information security to be the most balanced.

The managerial actions that a company takes are manifested in the various areas of the information security components, and the aim of these actions is to ensure that the information possesses all of the core characteristics. This relationship is illustrated in Figure 19. The figure includes the terms 'information security culture' and 'information security policy' also. These are discussed in the following sections of the work. They are considered important elements in the information security activities of a company.

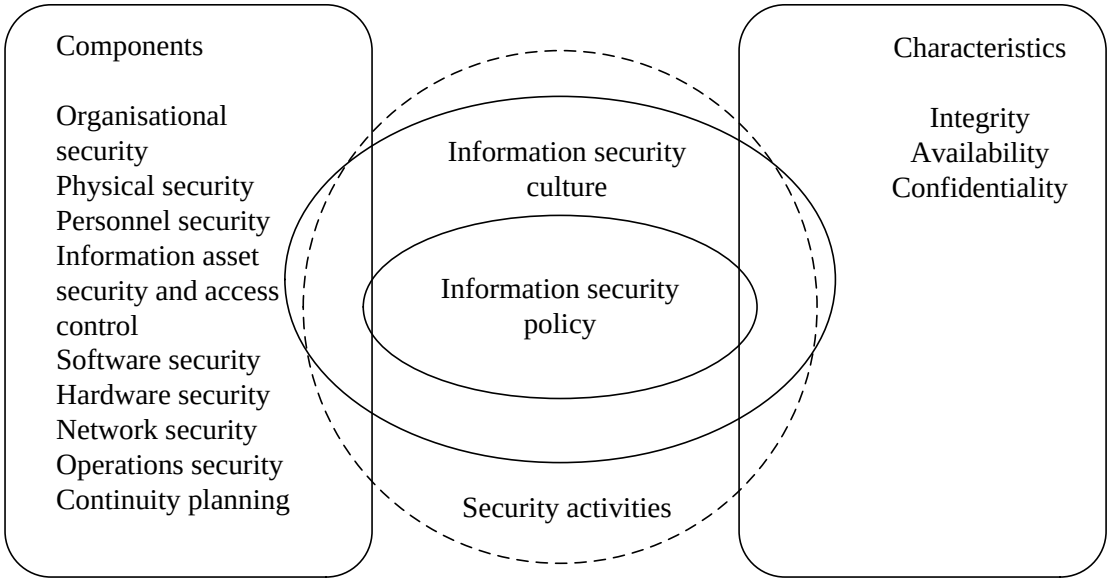

Figure 19: The relationships between information security components and characteristics

The first component listed in Figure 19, organisational security, includes the actions to plan, implement, and develop information security (VAHTI 2009). This component is very close to what Tipton and Krause (2004) call information security management. Organisational security utilises information security management models that represent several distinct approaches to organisation of information security. The roles, responsibilities, policies, and procedures of information security too are encompassed by organisational security. The management models and tools are discussed in more detail in the next section.

The second component of information security is physical security. Physical security is not merely a component of information security; physical information security can be considered as one aspect of the overall physical security of a company (Tipton & Krause 2004, VAHTI 2009). The securing of premises against intruders and a good and safe work environment are the main goals in work toward physical security.

The third component listed in Figure 19 is personnel security. Personnel security refers to the actions a company takes to recruit trustworthy workers as employees, to assign suitable roles to these people, and to train people to be aware of security threats and the protective measures that are in place at the company (Whitman & Mattord 2003, Tipton & Krause 2004, Peltier et al. 2005, VAHTI 2009, Crossler & Bélanger 2009).

Fourthly, information asset security and access control refer to the secure use of information systems and information assets (Dutta & McCrohan 2002, Tipton & Krause 2004, VAHTI 2009). Various confidentiality classes of information are established, and the classification is employed in restriction of access to include only the information a given person is authorised to use, for example, in information systems. Asset

classification is needed also for preparation of instructions and policies pertaining to handling of information. The classification is based on recognition of important information; if information or knowledge is not recognised as important, it does not get assigned an appropriate security class. This is one area of common ground between information security and knowledge management, where benefits can often be found from better recognition techniques.

The fifth, sixth, and seventh components – software, hardware, and network security – involve matters related to technical information security. For example, the software a company uses needs to be up to date, for avoidance of problems with commonly known technical exploits. Also the hardware the company uses need to be maintained properly, and it must be updated in a reasonable timeframe, to forestall problems of equipment malfunctions. Network security refers to the secure use of networks within and outside the company's boundaries (e.g., Tipton & Krause 2004, Clarke & Furnell 2007, Kumar et al. 2008, VAHTI 2009). These technical aspects are the ones that an average person thinks about when asked about information security and have received much attention also in the scientific literature. Therefore, this study does not concentrate on them.

The eighth component, operations security, refers to a secure work environment at the company, guaranteeing that information is safe wherever and whenever it is used. This is closely linked to technical security elements as much as to physical security (Peltier et al. 2005, VAHTI 2009). For example, backup routines are considered one aspect of operations security, for avoiding problems even if information is, for some reason, lost.

Continuity planning, the last component in the list, is, as physical security is, one aspect of a broader activity. From the information point of view, continuity planning refers to plans for uninterrupted operations of the company in mildly or even severely disruptive circumstances.

The components listed above describe in more detail the kinds of topics that information security management processes address. The management process binds these diverse components together under the guidance of an information security strategy and policies. The management process, however it may look, is aimed at promoting secure actions in the areas of the various components and documenting these actions within information security policy and procedures or handbooks.

In Figure 16, the components of information security are illustrated as forming one larger element that drives the information security policy, culture, and activities. The other driving element is the set of characteristics for information: integrity, availability, and confidentiality. This means that all activities driven by the information security components must address the three characteristics desired for information and somehow contribute to actualising one or more of them. When the activities are implemented and monitored, they influence the company's information security culture. Figure 19 presents the interdependencies of the individual components and characteristics.

Whether this entity composed of information security components and characteristics encompasses the concept of knowledge security, which is the topic of interest for the present study, is debatable. Knowledge security is presumed in Subsection 1.3.1 to emerge from the protection mechanisms targeted at knowledge. The security components in Figure 19 can involve also a security perspective on knowledge but only if this is taken into account by the management of the company in question. The components are described in the theory at a quite general level. Whether the focus in them is on data, or on information and knowledge also, depends on how security measures are taken by the company applying them and on what kinds of measures these are.

2.3.3 Information security management models

Information security management has its roots in computer security. However, the management perspective on information security too has had an essential role in the scientific discussion of information security, at least for the past decade (von Solms 2000, Whitman & Mattord 2003, von Solms & von Solms 2004a, Tsohou et al. 2010). The role of management in information security is very much acknowledged. Diverse management models exist, and, depending on the author presenting the model, there may be three to seven or more steps representing measures that information security managers should take to ensure information's integrity, availability, and confidentiality.

A very generic information security management model is presented in the standard for information security management systems (ISO/IEC 2005). The basic model is presented as involving four phases, which are given the generic names 'plan', 'do', 'check', and 'act'. This model is applied not only in information security management but also, for example, in quality management. It is illustrated in Figure 20.

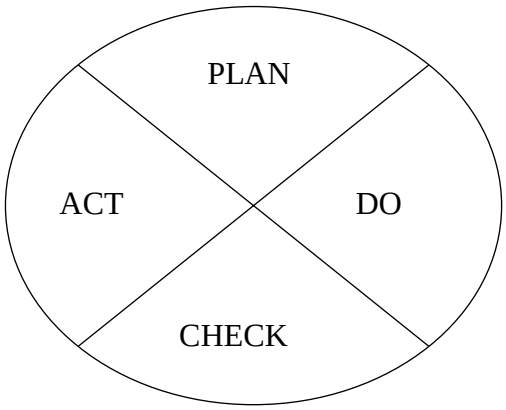

Figure 20: The information security management process (ISO/IEC 2005)

In the context of information security management, the planning phase depicted in Figure 20 includes the identification of important information assets and the planning of

security measures. The next phase is implementation of the plans. In the implementation phase, companies can utilise the various controls that are suggested in the standard. The check phase involves regular assessment of whether the plans are being implemented in the right way and whether the controls work or not. The results of these assessments can lead to changes either in the plans and policies or in the implementation of them. (ISO/IEC 2005)

The ISO information security management system model presented above is, again, quite generic and can be used for guidance in how to develop a working information security programme at a company. However, the standard model links many actions together in a single step of the programme: planning and developing policies are clumped together in one step, and the implementation phase covers actions of various types. This is why a security programme model that breaks the management process into more steps could be more useful. For example, Kairab (2005) includes seven elements in an information security programme. These are illustrated in Figure 21.

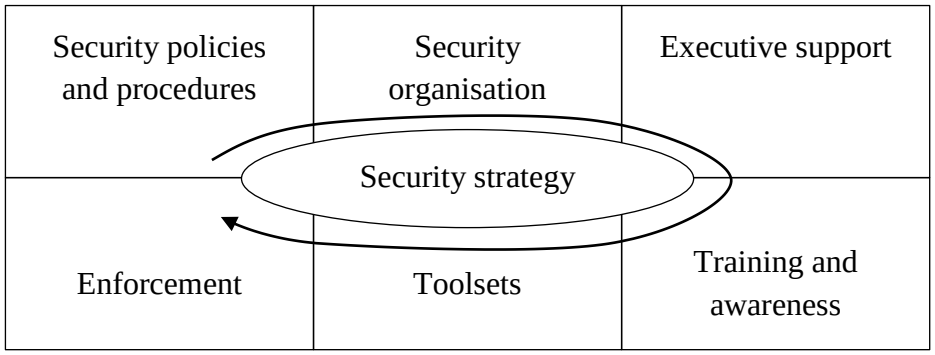

Figure 21: An information security programme (adapted from Kairab 2005)

Kairab (2005) gives the security strategy pride of place: it drives the rest of the programme illustrated in Figure 21. The security strategy consists of understanding the security risks that the relevant company is facing and developing the most cost-effective way to protect that company's information assets. The strategy should be formulated by key stakeholders in the company and driven by the needs of the business. In development of the strategy, critical data and applications have to be identified and their importance for the company's business assessed.

Kairab (2005) continues the security programme (Figure 21) with the development of security policies and procedures, the tools for implementation of the security strategy. The policies and procedures must also be in line with the overall strategy of the company and reflect the business goals set.

After the policies and procedures have been prepared, a security organisation needs to be established. The security organisation is a group who ensure that the information security programme is followed and maintained. This group's duties include updating

the policies, enforcing them, and scanning for new security issues that may emerge with changes in the company.

Executive support for the security programme as a phase refers to the general attitude of managers toward information security. The managers can make or break the programme with their attitude and actions. Setting a good example and extending the same information security rules to everyone working at the company paves the way for a successful security programme.

Training and awareness is the next element in the information security programme, according to Figure 21. People need to be regularly reminded of their roles and responsibilities related to information security. Companies can be very complex, and the roles of their employees vary a great deal, but the training and awareness initiatives must still address everyone at the company in a suitable manner.

The toolsets of the security programme bring in a technical perspective on security initiatives. This is the element that utilises, for example, the control lists of various standards that ensure adequate protection of technological systems. Many security checks can and should be automated (password strength control, system updates, etc.).

The last element in Kairab's (2005) security programme is enforcement. This means actively ensuring that the information security policies and procedures are followed. The toolsets mentioned above can form one mechanism for enforcement of the policies. Audits and reports on them are another: uncovering security concerns should lead to improvements in the security programme. Security assessments should always map back to the security strategy and to business needs. All security initiatives at a company need to be grounded in a business need and an identified risk.

Peltier and colleagues (2005) describe an information security management process that shows similarities with both of the models introduced above. They describe the information security policy as a central focal point from which all other activities in the process are driven. Figure 22 illustrates this process.

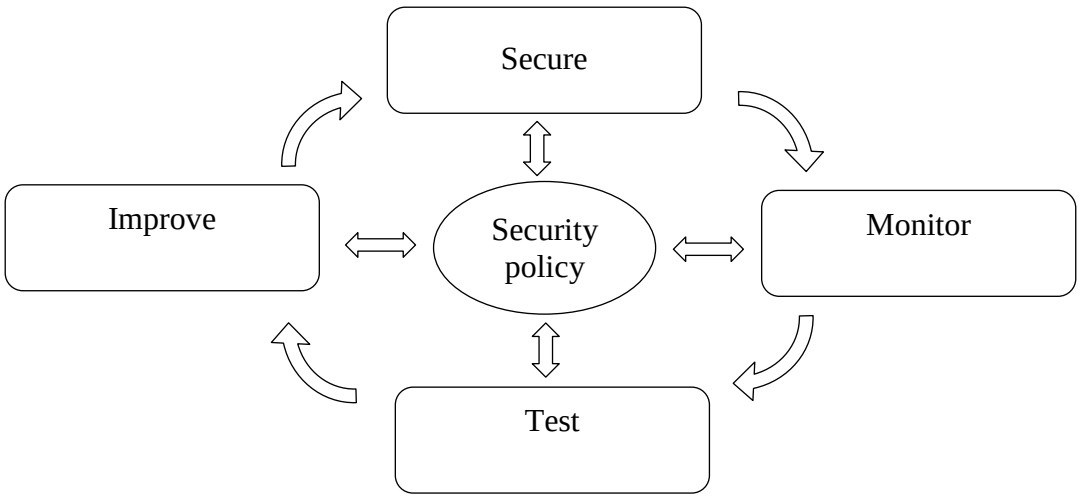

Figure 22: The security management process (adapted from Peltier et al. 2005)

In Figure 22, the security policy is illustrated as a central driver of the securing, monitoring, testing, and improvement phases in the information security management process. Although Peltier et al. (2005) do not elaborate on their illustration of the process, they emphasise many components that fall within the 'Secure' phase of the process. In this phase, multiple security components are brought together and the security policies implemented. All security activities need to be monitored, so that the current state of security is known. Through monitoring and active testing, the managers can plan for improvements in the security policies and in their implementation.

2.3.4 Risk management approaches to information and knowledge

Risk management is a very commonly used approach to information security. Assessing and addressing risks carries the information security management process forward to a tangible level of decisions (Whitman & Mattord 2003, Peltier et al. 2005, Wang et al. 2008). Managers need to identify risks before they can choose protective measures and determine the priority for each (von Solms & von Solms 2004a).

The process begins with asset valuation, determination of the value of individual knowledge and information assets (Gerber & von Solms 2001). With the threats to information and knowledge being of numerous types, they need to be used as input to calculations of risks (impact × probability) and then evaluated comparatively: which risks are to be addressed, and left unaddressed (Peltier et al. 2005)? There are some problems associated with this approach, however.

Risk assessments and calculations appear very precise. Every threat is reduced to a number and then compared to other numbers (Bojanc & Jerman-Blažič 2008). This process appears objective and robust; however, under closer examination, the robustness fades: risks are always assessed on the basis of intuition (Lacey 2010). Especially with immaterial cases such as knowledge leaks or loss, it is impossible to

precisely state a monetary value of the loss. Also, it is impossible to know precisely how probable the threat is. The intuitive estimate of both of these must add up to a guess (Gerber & von Solms 2001), a sophisticated one but a guess nonetheless.

If risk assessment is equivalent to guessing, are the managerial measures taken on the basis of the assessment really reasoned? And if they are, what is the reasoning behind them? One answer to this question is that documented risk assessment proves that many threats to the business have been recognised and evaluated. The assessment documents the choices made by the management, even if they are just guessing which threats are more severe than the others (Lacey 2010). The management need to be able to show that they have been diligent in their work (von Solms & von Solms 2004a). Even if weak, the assessment has value as evidence of the line of thought of the management.

The risk management perspective is brought in at many companies as an essential part of management. Neef (2005) claims that knowledge management tools and processes can be used effectively for corporate reputation and risk management purposes. His concept of knowledge risk management (KRM) constitutes the capture of knowledge related to any incidents that could possibly harm the company's reputation. The elements of a KRM programme include the following:

- A co-ordinated programme to ensure an ethical management framework in the company
- A system to measure the managerial initiatives taken at the company
- Open reporting on financial and non-financial subjects, to ensure measurable figures for input into management
- An integrated KRM process that leverages best-practice risk-related and KM procedures and systems

These elements together form an integrity framework that helps the company to capture and use knowledge that could prove helpful for preventing reputation incidents (Neef 2005).

Why, then, is risk management a good approach to security of knowledge? Risk assessments usually concentrate on known risks that are recognised on the basis of standards and best practice. However, the greatest risk lies in the unknown that cannot be foreseen but is easy to predict after it has been actualised once (Taleb 2008). No matter how systematically a company performs risk analyses, those analyses cannot provide information about unknown threats. This is why risk management needs to be complemented with security strategies that do not rely purely on reactive response to established risks. In contrast, proactive security thinking requires many dynamic capabilities from a company, since proactive measures need to change rapidly with the environment. The KRM framework is one step toward that proactivity, with the aim of open reporting.

Kayworth and Whitten (2010) link the risk management approach and the strategic information security approach together in their framework designed to foster effective

information security in companies. This framework is depicted in Figure 23. The idea with this framework is to acknowledge that information and knowledge risks can be managed via more than just technical and mechanical solutions. Integration of the organisational controls such that the company's operations do not cause risks themselves is the first step. The social alignment of risk management mechanisms through awareness training and cultural mechanisms is also important. Of course, neither should the technical side of risk management be forgotten (Kayworth & Whitten 2010).

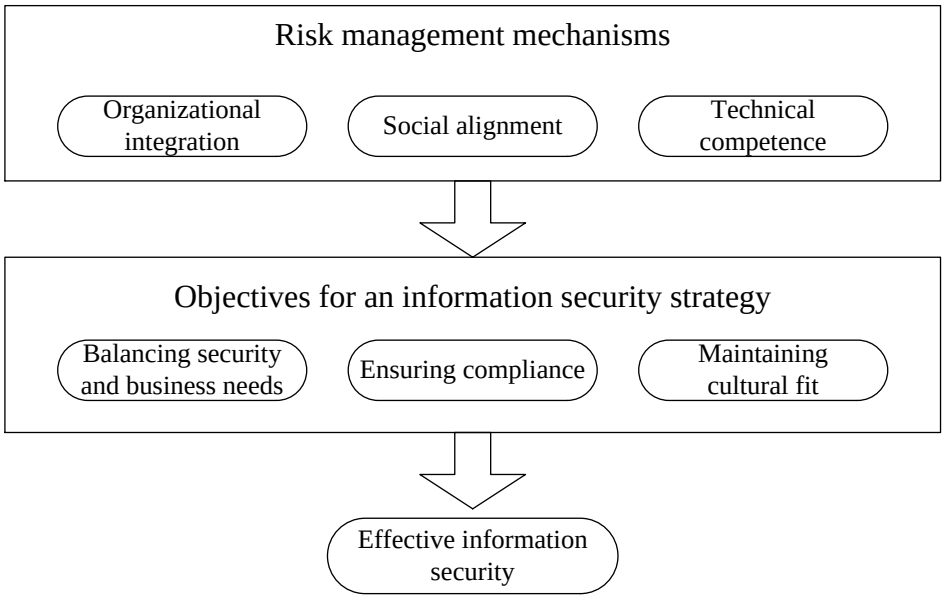

Figure 23: The risk management and information security strategy framework (figure from Kayworth & Whitten 2010)

In pursuit of effective information security, Kayworth and Whitten (2010) describe three key objectives that a company's information security strategy must meet if it is to succeed (see Figure 23). First of all, they emphasise that security needs and business needs need to be balanced. Information security is, most of all, a compromise between, at one extreme, total security but no business and, on the other hand, open business with no security. An appropriate balance between the two has to be found. Risk analyses are the tool for deciding which risks are worth taking and which are too great to bear. (Kayworth & Whitten 2010)

Ensuring compliance is another objective that Kayworth and Whitten (2010) set for an information security manager. They argue that, by making information security easy for the employees, a company steers a course for success. In this context, 'a security department that tries to control everything will fail'. Enough flexibility and a good awareness programme help to build a culture of information security within a company. The authors argue that a strong culture motivates people to comply with information security guidelines better than strict controls do (Kayworth & Whitten 2010).

Risk management as an approach complements the other ways of approaching information security management with in-depth examination of threats and their consequences. Information security is an activity addressing the threats to information in a company. The risk management perspective gives tools to assess and compare the individual threats that need to be addressed. A company faces many risks, not all of which can be addressed in equal manner. The risk management tools provide ways of prioritising the risks and thus selecting those security measures that benefit the company most. This prioritisation is part of the planning and implementation steps in the information security management models presented in the previous section.

2.3.5 Information security policy

As described in Subsection 2.3.3, security management models position the security strategy or policy as a key point for security measures. In this study, differentiation between information security policy and strategy is not necessary, because the ultimate goal for both is the same: to document a plan of action for information security measures. For the sake of clarity, the term 'information security policy' is used here, since this is the term more commonly used. In this section, the term is examined, to reveal what various authors mean by it and how they address its role.

The word 'policy' refers to a plan of action adopted or pursued by a business or other organisation (*Collins English Dictionary* 2006). By this definition, an information security policy refers to the plan of action for the securing of information in a company. This general definition does not, however, give much information on the level of detail or abstraction of the plan. Therefore, field-specific definitions for information security policy are presented below.

Shorten (2004) states that an information security policy is the foundation on which all security is built. The policy should cover various themes in sufficient detail to state what should be done, whilst information security procedures state precisely how the actions described in the policy should be implemented. In all, Shorten (2004) lists 21 issues that should be addressed by the policy, some of them more specific than others. In short, the policy tells staff what they may, may not, or must do, alongside what their responsibilities are. The process of writing and accepting the policy includes the security professional writing the policy, the CEO and board of the company approving it, and the CEO validating the policy by signing it.

According to Barman (2001), the information security policy is a high-level plan that describes the goals of information security procedures. He emphasises the role of security policies as blueprints for security. Without these blueprints, constructing security is not easy and there is a risk of efforts toward it not being consistent. Barman also reminds the reader that security policies are a tool to mitigate liability if something goes wrong. This emphasises the role of the top management in the making of

information security policies. Barman cites three main areas that these policies should cover: access control policies, external access policies, and user and physical policies. He stresses that information security policies need not take the form of a single document; a collection of separate policy documents, for different areas, should suffice as well.

Peltier et al. (2005) have a different approach to information security policy, in that they describe information security policy as a collection of company-wide policies in three distinct tiers. Their instructions on how information security policies are to be documented and the information security management process managed are most comprehensive and clearly intended for large corporations. Although the matter of company size is not mentioned, the suggestion of having more than 10 members on the information security committee or writing 11 company-wide tier-1 policies supported by tier-2 and tier-3 policies implies a large target company. The authors recommend a strict hierarchy separating the policy documents and intend that they be very detailed.

The authors cited above (Barman 2001, Shorten 2004, Peltier et al. 2005) define the information security policy as a general document that clearly states the goals for information security at a company. However, in addition to general guidelines, the authors expect the document to include detailed instructions on various technical and non-technical subjects. While the authors begin their work by using the term 'information security policy', the word becomes plural, 'policies', quite quickly. A distinction between documents at different levels is not made clear, with only Peltier and colleagues (2005) clearly instructing in different levels of documents and abstraction, referring to these as different tiers of information security policies. Other authors write about policies, procedures, guidelines, standards, etc. that complement the information security policy.

The definition of 'information security policy' depends on the person using the term. As a synthesis of the definitions above, information security policy as referred to in this study is considered *a high-level document that states the information security strategy of the company*. The word 'strategy' here refers to the basic idea and goals of the information security efforts. This document lists the information assets of the company (what is protected), the responsibilities of the employees (who is to be protected), and the overall plan as to what measures are in place to protect the information (how protection is carried out). To complement this strategic document, information security procedures and guidelines are needed, so that technical solutions and work procedures can be streamlined to meet the needs of security. The lower-tier policies are referred to with the terms 'procedure', 'guidelines', and 'handbook'. The term 'information security strategy' is avoided, because it is not commonly used in the information security management literature. Although there are authors who call for a strategic approach to information security (e.g., Kayworth & Whitten 2010), the term 'strategy' is not commonly used in connection with information security management. The

information security policy document often serves the purpose of an information security strategy in a company, if a policy is documented at all.

Information security policies do not, in themselves, necessarily meet the need for information security in companies. When an information security policy exists and the company has staff to enforce the policy, employees still do not necessarily comply with the policy (Siponen & Vance 2010). Non-compliance is a major issue in information security, and many studies show how motivating employees to follow the information security policy proves a real challenge for companies (e.g., Myyry et al. 2009, Siponen & Vance 2010, Bulcuru et al. 2010, Smith et al. 2010, Spears & Barki 2010). The strength of the information security culture is seen as one possible factor in how well the employees comply with the information security policy (Thomson et al. 2006, Boss et al. 2009, Siponen & Vance 2010, Van Niekerk & von Solms 2010). This connection between the information security culture and information security policy resembles that between knowledge management efforts and the company's organisational culture. The following section examines culture more closely, for insight into what cultural elements are common between information security management and knowledge management.

2.4 Culture

The background theories of this study assume that organisational culture is a context wherein knowledge management and information security management take place. This context also has an impact on the success of knowledge management and information security management efforts. Accordingly, organisational culture can serve as one route to implicit awareness of the value of knowledge and of its protection.

In this section of the work, the concept of organisational culture is introduced first. Then, the parallel term to 'information security culture', 'safety culture', is examined for analogies between the safety culture for physical phenomena and information security culture. The discussion of culture in knowledge management theories is examined also.

2.4.1 Organisational culture

Organisational culture is a concept that emerged in scientific literature as early as in the 1950s (Denison 1996, Guldenmund 2000). The term became strongly embedded in the scientific management literature only in the late '70s and early 1980s (Pettigrew 1979, Potter 1989, Denison et al. 2003, Paalumäki 2010). Before the '80s, most research in this area employed the term 'organisational climate'. One approach to linking these concepts together is to define organisational climate as something that emerges from the organisational culture (Wallace et al. 1999, Guldenmund 2000). This would mean that organisational climate is a reflection of the organisational culture, which is a more

embedded construct and harder to research than organisational climate. The challenges of studying organisational culture and its effects on an organisation are widely acknowledged (Denison et al. 2003, Milne 2007, Niels 2008, Paalumäki 2010, Rai 2011). Culture is defined in many ways, so the term is elusive and difficult to study and measure. Some of these definitions are presented in the discussion that follows, to create an understanding of what various authors mean by the term 'organisational culture'.

According to Schein (1984), organisational culture manifests itself on three levels: the level of artefacts, the level of values, and the level of beliefs. Other authors distinguish more layers within the layer Schein calls artefacts, (e.g. Guldenmund 2000) such as organisational stories. These layers, however, can still be mapped back to the three levels of organisational culture presented by Schein (1984), which are depicted in Figure 24.

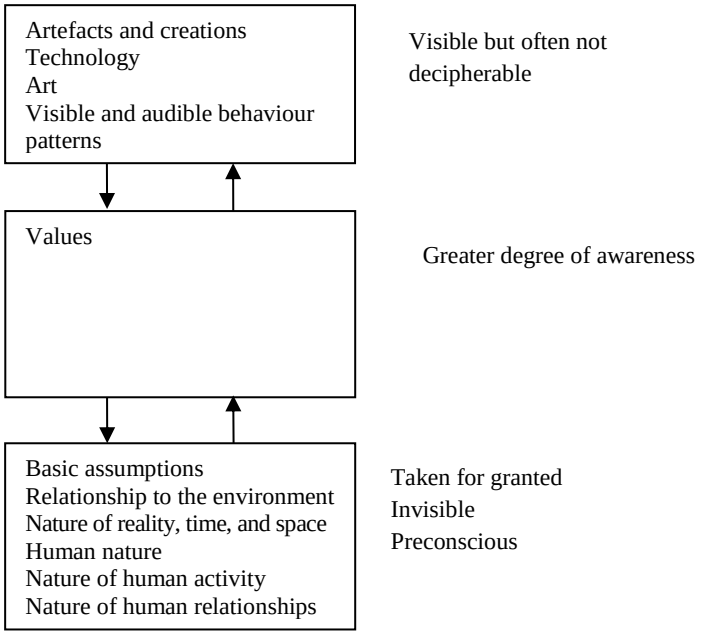

Figure 24: The levels of organisational culture (application of Schein 1984)

The highest level in Figure 24, artefacts, is the visible level of culture, which is easy to examine but hard to interpret (Schein 1984). For example, the office space and work materials of an organisation can be easily examined, while understanding how the office construction or the materials and instructions reflect the organisational culture can be difficult. For an understanding of the artefacts, the values of the organisation need to be examined. This can be done, for example, via interviews with members of the organisation and analysis of the contents of the artefacts. However, even this analysis does not provide full understanding of why those in organisations behave the way they do. To gain true insight into the culture, one must examine the level of assumptions and understandings (Schein 1984). This is easier said than done, however, since the shared assumptions are not explicitly expressed and change slowly over time.

Hofstede (2001) has studied culture mainly from the perspective of nations, but many of the ideas about culture as a national phenomenon can be transferred to the context of organisations. Where Schein (1984) distinguishes between different layers of consciousness, Hofstede (2001) examines layers of mental programming from the universal down to collective and individual levels. He argues that on the universal and individual level the mental programming is bound to human nature and our heritage, but on the collective level it is to a large extent learned. Therefore, the collective level is the level of scholarly interest here. Organisations are situated at the collective level in Hofstede's categorisation. He defines culture as a phenomenon born in the interactions of the values, practices, rituals, heroes, and symbols of people's collectivity. Culture thus requires a collective, an organisation of some sort, to exist. (Hofstede 2001)

Hofstede's way of conceptualising culture has been subject to criticism (e.g., Baskerville 2003, Hofstede 2003) and this critique in part underscores the difficulty of grasping and studying a phenomenon that is deeply embedded in people's minds and behaviour. Culture is defined differently and operationalised in studies differently. Hofstede (2003) argues that there exist several characteristics by which one can distinguish among national cultures when the comparison encompasses enough nationalities. This raises the question of whether this holds true also in the case of organisations: can types of organisational cultures be found when enough organisations are studied? In his work, Hofstede (2001) points out the difficulty of researching culture without affecting it: how to measure the values of a person without injecting the values of the researcher into the results. This may be one reason that organisational climate is still oftentimes studied alongside organisational culture (Riivari et al. 2012): it may be easier to measure with quantitative methods or through observation.

Guldenmund (2000) defines organisational culture by way of seven characteristics that are a reflection of the previous definitions presented above for organisational culture:

- It is a construct rather than a concrete phenomenon.
- It is relatively stable; i.e., it changes slowly over time.
- It has multiple dimensions.
- It is shared by groups of people, and it is holistic. This means that one must also examine the way the components or levels of the culture construct the culture.
- It consists of various aspects; this means that several, different cultures or climates can be distinguished within an organisation – e.g., a service climate or a safety culture.
- It has many layers, and the more 'superficial' the layer, the easier it is to change.
- It is functional. One simple and well-known definition of culture is 'the way we do things around here'. That effectively captures this functional aspect.

Overall, organisational culture is a 'relatively stable, multidimensional, holistic construct shared by (groups of) organisational members that supplies a frame of reference and which gives meaning to and/or is typically revealed in certain practices', Guldenmund 2000).

Organisational stories are mentioned as one layer or element of the organisational culture (Guldenmund 2000). Although organisations are unique, there are, according to Martin et al. (1983), typical stories that exist with slight variations across multiple organisations. These stories can be either positively or negatively oriented. Positive stories depict heroes who have somehow saved the organisation, overcome exceptional burdens, or showed unexpected devotion to the organisation. Negative stories depict situations wherein the management did not follow the guidelines or in which they acted unreasonably. (Martin et al. 1983) The power of stories lies in the efficient spreading of what constitutes desirable and undesirable activities – in other words, the spreading of values.

The stories of culture represent a way in which each organisation can distinguish itself from others. Although the stories are similar in structure, each is unique in how it represents the culture of the organisation from which it is born . (Martin et al. 1983) An interesting way of looking at organisational stories is to contrast them to Schein's (1984) levels of organisational culture. An organisational story can be an artefact (Schein 1984) when inscribed in explicit form and distributed through the organisation in one way or another. Many success stories are, or could be, used as artefacts to help people identify as members of the organisation. Negative stories do not necessarily appear in explicit form. If they are spread only with speech, can they be considered artefacts? Rather, they are at the level of values and assumptions; for example, they convey how the management follow the explicit values of the organisation. In this way, negative stories give one reflection of the lowest level of the organisation's culture, the shared beliefs and assumptions.

General agreement on the actual definition of the term 'organisational culture' is lacking (Drumm 1991 in Maier 2010). In summary of the above, organisational culture can be described as a phenomenon that has many layers. It is elusive and therefore difficult to study. This is why research on organisational culture has concentrated more on the more easily measurable reflection: organisational climate. The culture, however, is more than just a driver of the climate or work atmosphere. For example, the concept of ethical culture can be defined as 'those aspects and conventions of behavior that encourage the organization to operate in a sustainable way or deter it from doing so' (Riivari et al. 2012). If we excise the ideas of ethics and sustainability from that definition, organisational culture could be defined as the aspects and conventions of behaviour that encourage the organisation to operate in a desirable manner or deter it from doing so. The values layer of organisational culture (e.g., Schein 1984, Hofstede 2001) denotes the presence of a desired or desirable line of action in the organisation. Accordingly, culture is something that directs the behaviour of the individuals in the organisation, as much as the behaviour of the organisation as a whole. In the following sections, organisational culture is examined from different perspectives, of safety, security, and knowledge management.

2.4.2 The knowledge management perspective to organisational culture

In Section 2.2, organisational culture was considered as a driver or context for the knowledge management initiatives. The main theories of knowledge management and approaches to it consider culture an important element in the success of knowledge management initiatives. The success of these initiatives is dependent in part on how well employees adopt new ways of working and communicating (Bock & Kim 2002, Chua & Lam 2005, van den Hooff et al. 2012). Studies have shown that there are various cultural factors that can either support or complicate the knowledge management efforts (e.g., Bock & Kim 2002, Ipe 2003, Awad & Ghaziri 2004, Suppiah & Manjit 2011).

Although the presentations of the various approaches to knowledge management are expressed in positive form, the outcomes of knowledge management are not always purely positive. For example, Chua (2009) lists several problems that have arisen from knowledge management initiatives that have been considered successful in light of the metrics in use at the company in question. There is a tendency for companies to approach a problem with a solution that has worked before. Chua calls this the competency trap. In this trap, fixation on set knowledge management procedures and established knowledge repositories may lead to diminished problem-solving ability. Another problem listed by Chua is that communities of practice may end up as communities centred on an inner circle with its dogma. Also, measurement associated with the knowledge management initiative may lead to opportunistic behaviour and even ethically questionable practices. All of these problems may be lurking within a seemingly successful knowledge management implementation. (Chua 2009)

The organisational culture may be so strong that establishing change at all levels of action is difficult. In the above examples Chua (2009) provides, many problems may be caused by the knowledge management initiative having succeeded on the level of artefacts but failed on the deeper levels of culture. This leads to the appearance of changes in actions whilst people are, in fact, still doing things in the old way and just applying the knowledge management practices on the level of artefacts, such as reports (Chua & Lam 2005). In this case, the organisational culture complicates the knowledge management initiative instead of supporting it.

Some studies and authors emphasise the positive impact of a ‘knowledge culture’ on a company’s knowledge management efforts (Maier 2010, p. 132). Organisational culture can support knowledge sharing (Davenport & Prusak 1998, Holste & Fields 2010, Suppiah & Manjit 2011) and knowledge creation (Nonaka & Takeuchi 1995). However, the literature does not always elaborate on how this beneficial knowledge culture is created. Some say the culture cannot be changed intentionally, while others believe that changes can be made and knowledge management initiatives can be a way to establish

changes in the organisational culture (Maier 2010). In any case, culture is a major driver for knowledge management efforts. It needs to be taken into consideration from the perspective of the ways in which it can cause complication but also in terms of how it can support the knowledge management efforts undertaken in a company.

2.4.3 Safety culture

A sub-culture of a company's organisational culture that is related to security issues is the safety culture. Occupational safety literature concentrates on the physical risks that a company deals with and aims to prevent via the safety culture. In this, a company's safety culture is analogous to the information security culture of the company.

In a parallel with organisational culture, safety culture research began as safety climate research (Clarke 2000). Safety climate scores were expected to reflect the accident rates in companies, since the safety climate acts as a frame of reference for employee behaviour (Zohar 1980 in Grote 2007). Correspondingly with safety culture, the safety climate can be seen as reflecting the underlying safety culture, as illustrated in Figure 25.

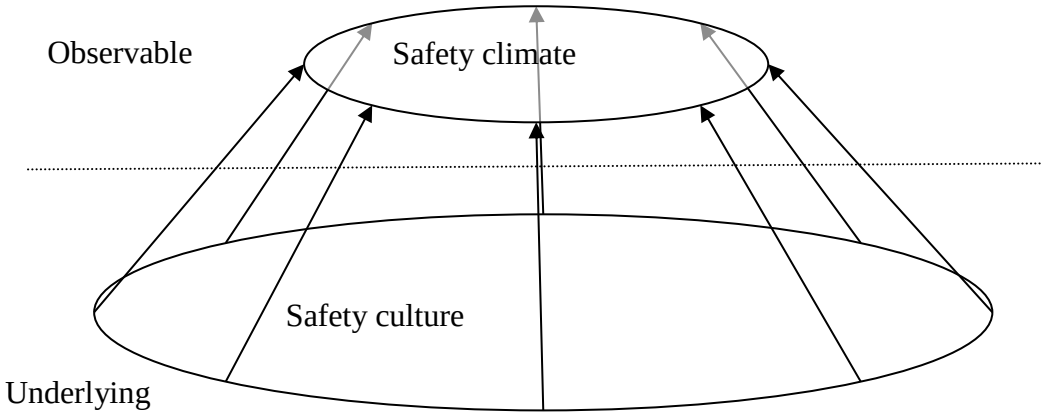

Figure 25: The relationship between safety culture and safety climate

In Figure 25, the link between the underlying safety culture and the observable safety climate is illustrated as an incomplete reflection. The culture is reflected by the climate, but the climate is not a complete representation of the culture; i.e., there are elements of the culture that are broader than their reflection in the safety climate.

Cooper (2000) defines the safety culture as a sub-culture to the organisational culture except when the organisation operates in a high-risk industry, in which case the safety culture would be the dominant culture in the organisation. Either way, the safety culture is not homogenous throughout an organisation. For example, individual departments and teams may have their own understanding of the prioritisation between safety regulations and production goals. Priorities do vary in line with risk profiles, but

differences in understanding across departments lead to differences in the (plural) safety cultures in the organisation. (Cooper 2000)

Grote (2007) sheds new light on the concept of safety culture, which is often considered quite superficially as referring to the safety-promoting norms and attitudes shared by the members of an organisation. According to Grote, a positive safety culture means centralised values and norms that serve as a strong basis for the choices people make when they work autonomously and in a decentralised manner. Culture is seen more as a means of providing sufficient co-ordination and integration of otherwise autonomous agents than as the general assurance of safety as a core value. (Grote 2007) Cooper's (2000) point that each department could end up with a different safety culture is addressed in this approach, according to which key values and norms need to be actively driven in the organisation, so that they build a homogenous basis for the various safety cultures.

Measuring the elements of a safety culture is tricky, since culture is a complex construct, with many elements that are difficult to measure. The elements are similar to those of organisational culture as introduced in the previous section. The organisation creates safety, and this is only one aspect of its actions. Through understanding of the operations of an organisation, the safety needs can be more precisely determined. If there are multiple goals, some may conflict with safety goals (Reiman & Oedewald 2010).

Measuring the effectiveness of a safety culture is more easily said than done. One metric commonly used is the accident and incident rate. There is one big risk, however, connected with this: accidents and incidents may be hidden. The accident rate reflects the safety culture but also the ability of employees to cover up minor accidents. People may feel that, in the eyes of the company, an incident never happened if it was not reported. Such an attitude does not foster a proactive safety culture, which benefits from all information about accidents, incidents, and near misses.

One factor in a safety culture is the communication and use of safety incident information (Díaz-Cabrera et al. 2007). A simple and common-sense-based way of interpreting this factor's effects is that people are motivated to report safety incidents if the reports really are used for improvement. This may also require that employees participate in the analysis of safety reports and in the improvement efforts. In some organisations, the managers and other workers may differ greatly in their understanding of safety (Harvey et al. 2001). This difference in approach could lead to a situation wherein employees feel that the management are interested only in the safety report numbers, not in the phenomena behind them. This is why communication about how the safety reports have been used in decision-making is very important.

In one view, '[o]rganizations are defined by what they ignore – ignorance that is embodied in assumptions – and by the extent to which people in them neglect the same

kind of considerations' (Weick 1998 in Reiman & Oedewald 2010). Safety is always something that is defended against recognised risks. Organisations need to be humble and admit that not all risks can be recognised. Accordingly, actions should be directed at recognising risks as early as possible. A good safety culture involves maintaining a healthy attitude of humility throughout the organisation. For this, the above-mentioned measurements need to support the safety culture.

2.4.4 Information security culture

Information security culture and awareness is mentioned in many articles as one key driver for a good level of security (e.g., Schlienger & Teufel 2003, von Solms & von Solms 2004b, Thomson et al. 2006, Van Niekerk & von Solms 2010). As knowledge is to a large extent impossible to keep secure by technical means, the basis for knowledge security lies in the security culture and managerial actions. This is why information security culture is an important background concept for knowledge security.

According to Martins and Eloff (2002), information security culture refers to the dominant understanding of how information security principles are manifested in the daily operations of an organisation. The culture points to what kind of employee behaviour is acceptable and encouraged. (Martins & Eloff 2002) von Solms (2000) agrees to a great extent with the above definition. According to her, the information security culture must support the instructions and procedures of the organisation, so that information security becomes a natural part of daily routines (von Solms 2000). All these authors indicate that information security culture can be consciously developed through direction of employee behaviour toward the desired direction (von Solms 2000, Martins & Eloff 2002). In a similar but slightly narrower approach, Schlienger and Teufel (2003) define information security culture as encompassing all of the socio-cultural methods that support technical information security. Through the implementation of these, information security becomes part of daily operations (Schlienger & Teufel 2003). These definitions show that information security culture studies, in contrast to safety and organisational culture research, are not an offshoot of information security climate research. One explanation for this lies in the fact that the field of information security culture is much younger than the others considered.

Indeed, information security culture is a relatively new concept. While definitions for it vary little, definition of the concept is complicated by the use of parallel terms. 'Information security awareness' (e.g., Siponen 2000, Tsohou et al. 2008) and 'information security obedience' (Thomson et al. 2006) are examples of terms with parallel definitions. Distinguishing the terms from each other is difficult; for example, Ruighaver et al. (2007) and Schlienger and Teufel (2003) use the term 'security culture' to mean roughly the same thing the others mean by 'information security culture'. This may be a result of the publication venues and the tradition of the research field: in

information system research, repeating the word ‘information’ in every term is not considered necessary by all authors.

Common to all of the sources cited above is the notion that information security culture intensifies the implementation of technical information security initiatives. According to them, a good information security culture encourages the employees to obey the security instructions because it helps them understand the reasons for the instructions.

Ruighaver and colleagues (2007) have a different view. According to them, an approach of this kind limits the information security culture to only a small part of information security. Furthermore, it seems to confirm the old view that information security is mostly a technical issue. They emphasise that information security is mainly a concern of the top management and that the information security culture reflects the degree of success of the management in addressing this concern. The authors stress that one should not attempt to create an information security culture. Instead, the tools and policies of the organisation should be adapted to the dominant information security culture. (Ruighaver et al. 2007) This approach reflects the fact that it is much easier to affect the procedures and tools than the culture. However, the authors do not fully address the problems with changing a poor security culture.

The information security culture can be considered a sub-culture of the organisational culture. It encompasses the attitudes and assumptions of the employees about information and the information security rules and policy. At this juncture, it is necessary to stress that the term ‘information’ here is used in a general sense, to cover all: data, information, and knowledge. The information security policy of a company can be seen as an artefact of the information security culture.

2.4.5 The perspectives of culture

In summary of the previous sections, the organisational culture and the security culture as a sub-culture are drivers that to a large extent determine how people approach the activities they are expected to perform. Several components and layers of culture are identified, as are several effects of sub-cultures. Culture has also been defined on several occasions as elusive and difficult to measure; nonetheless, it needs to be managed if the company wishes to strive for good results (e.g., Denison et al. 2003, Milne 2007, Niels 2008, Paalumäki 2010, Rai 2011). In Figure 26, the perspectives on organisational culture presented in this study are summarised.

Figure 26: Multiple perspectives on culture

The general management perspective on organisational culture depicted in Figure 26 is presented in Subsection 2.4.1. Organisational culture is considered a phenomenon that has multiple layers and one that can be managed through exertion of an influence on these layers. The culture is fairly stable, however, which means that change takes place slowly over time (Schein 1984, Denison 1996, Guldenmund 2000). Organisational culture can be approached, for example, from the point of view of a narrative (Jill & Carroll 2010) or metaphorically, with the organisation being compared to a group of animals (Line 1999). The various metaphors of culture aid in understanding the individual aspects of the operations of a company, though use of only a single metaphor can mislead a manager into simplifying the complexity of the company too much (Morgan 2006).

The knowledge management perspective on organisational culture is presented in Subsection 2.4.2. The organisational culture is considered one driver for knowledge sharing and management (e.g., Bock & Kim 2002, Ipe 2003, Awad & Ghaziri 2004, Suppiah & Manjit 2011): the knowledge management perspective on organisational culture implies that culture can support knowledge management activities or hinder them, depending on the type of the culture.

The safety culture perspective in Figure 26 is introduced next, in Subsection 2.4.3. The discussion of safety emphasises the connection between the safety culture and safety climate: the climate is easier to measure and affect than the (more stable) culture. Safety culture literature discusses the handling of incidents as one indicator of the climate. The attitude of the company toward safety incidents has a crucial role in the development of

the culture (Harvey et al. 2001, Reiman & Oedewald 2010). A safety perspective on organisational culture thus involves considering attitudes as a key driver for the culture.

The information security culture perspective in Figure 26 is presented in Subsection 2.4.4. Literature on information security culture seems to emphasise employee behaviour perspectives, with the driver for information security culture rooted in the processes of the company and their implementation (Martins & Eloff 2002, Albrechtsen 2007, Bulcuru et al. 2010). Employees' awareness of information security risks and their attitudes toward the risks is another important driver for the culture.

Each of the perspectives on organisational culture or its sub-cultures discussed above brings its own approach to the elements of culture. Organisational culture is layered, and this layered nature should be considered when it is studied. Changes in one layer may lead to a false assumption that all the layers have changed and, thereby, that the culture has changed. The changes in the lowest layers occur slowly, even though the artefacts can be changed quickly. The lens of organisational climate offers one way to examine the culture. While it is not a complete reflection of the culture, it can be a route to finding the cultural elements that merit closer examination. The organisational culture is reflected in people's behaviour and attitudes. Through changes in behaviour, the culture can be changed, but, also, slowly changing the culture changes behaviour. Examining its organisational culture through metaphors can help a company to notice problematic aspects of its culture, as long as the metaphors do not oversimplify matters. All these elements may be useful in the analysis of the concept of knowledge security.

2.5 Summary of the theoretical background

This chapter has presented the two main streams of theoretical literature that prompted the research questions for this study. Even the concept of knowledge alone can be defined in many – quite different – ways, and the chapter provides some background on how the concept is interpreted in this study. Knowledge is defined here as a concept that *is embedded in people and their experiences. It is manifested in social interactions and in situations wherein people use their skills and experiences to solve problems and create new knowledge. Knowledge is embedded in people's tasks, roles, and routines, along with being embrained in their abstract understanding.*

The perspectives on recognising, codifying, sharing, and creating knowledge as presented above can be summarised as forming the activity of knowledge management. Figure 27 sums up the various perspectives on knowledge presented in Section 2.2. There are, of course, numerous other angles of approach to knowledge management, so Figure 27 is by no means an all-encompassing illustration of knowledge management. Instead, it is a summarisation of the perspectives that are relevant for the examination of knowledge that we undertake from the standpoint of security.

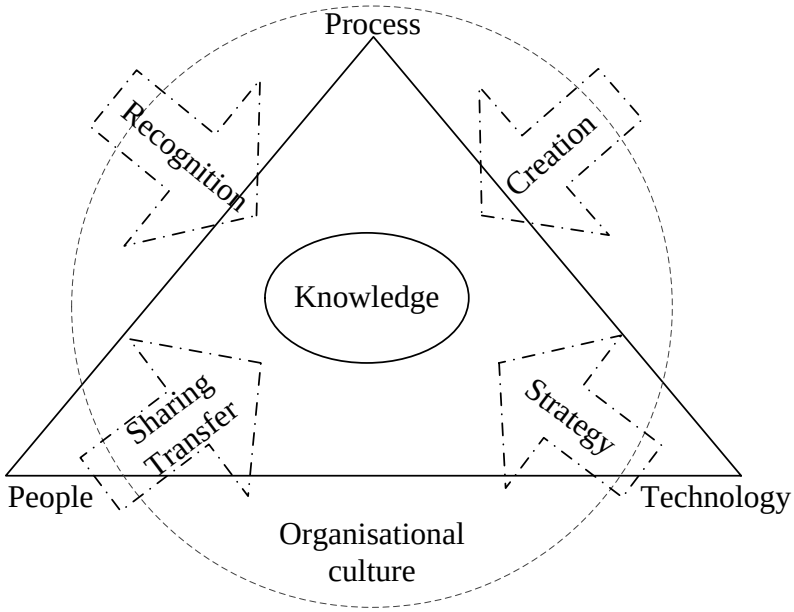

Figure 27: Knowledge management perspectives on knowledge

Knowledge recognition is the first perspective illustrated in Figure 27 and a good starting point for knowledge protection and security activities. Recognising what knowledge is important for the company and valuable for its business is a prerequisite for the activities that follow. Knowledge recognition has been studied from many perspectives, and still is (Prahalad & Hamel 1990, Barney 1991, Wilson 1994, Drott 2001). The main goal in knowledge recognition is to identify the knowledge of the employees as an asset to the company and recognise the value of the various knowledge assets. Knowledge that is needed for decision-making in the company is considered especially important in this study, since a company's operations grind to a halt quickly if this knowledge is not present and up to date.

The next perspective illustrated in the figure is that of knowledge creation. Creating knowledge *per se* is not important from the security point of view, but understanding how knowledge is created leads to understanding of where knowledge resides. This should assist in targeting of security activities and also in recognition of knowledge that is valuable to the company. Knowledge creation processes do not just create knowledge; at the same time, they utilise the existing valuable knowledge of the company.

In Figure 27, knowledge recognition and knowledge creation are mapped as closest to the process dimension of knowledge management. This does not mean that the other approaches do not involve processes; they are simply more human- or technology-oriented than are the others. The general approach with its human, process, and technology elements reminds us that all of the processes have a human and technology dimension. The three dimensions, or factors, as Awad and Ghaziri (2004) term them, are intertwined and often inseparable from each other. This is why the shape of a triangle works well in illustration of the approaches to knowledge management.

In addition to recognition and creation, the strategy for knowledge management needs to be considered, as Figure 27 suggests. Codification and personalisation (Hansen et al. 1999) are two strategies aimed at further availability of knowledge, and in this they are a seed for making that knowledge secure. This is one example highlighting that the security measures companies use are by no means separate from other practices in the company. A knowledge codification project may be justified in terms of gains in efficiency or time-saving effect. A side product of it may be increased availability of knowledge from the security point of view. However, the security angle needs to be taken into account in initiation of knowledge management projects such as codification, to ensure that the security impact of that project is not harmful for the company on account of, for example, decreased confidentiality of important knowledge.

The last perspective illustrated in Figure 27 is that of knowledge sharing and transfer. Processes of sharing and transferring knowledge too must be understood when knowledge is examined from the security perspective. Knowledge is not static, and security efforts need to embrace this fact. Knowledge is in many cases manifested in people's communication and collaboration, and, therefore, sharing and transfer of knowledge are essential if the company is to gain advantage from knowledge and create new knowledge. However, the grounds and justifications stated for knowledge sharing need to be in line with the security needs of the company.

Knowledge management theories tend to emphasise the good things that companies can achieve by adopting the various KM practices. Free knowledge sharing and the idea of creating a culture of knowledge sharing and creation may have its risks. Some of these are connected to people being fixated on one way of operating and thereby abandoning any creativity in the use of knowledge. Other risks may stem from lack of recognition of what knowledge one should share, with whom, and how. Yet more risks may be created through lack of recognition of important knowledge that must stay inside the company.

Knowledge recognition is the first step in addressing these risks. As we have noted above, recognition of important knowledge is not very well addressed in the knowledge management literature. Once the important knowledge is recognised, it is possible to consider a strategy to manage it, share and transfer it, and nurture it to create new knowledge. All of these, however, need to be done in a fashion that does not compromise the knowledge.

The information security perspectives on information, and knowledge along with it, are depicted as tools and characteristics. Figure 28 summarises the various approaches of information security as a combination of integrity, availability, and confidentiality and management tools such as information security policy, awareness training, and risk assessment.

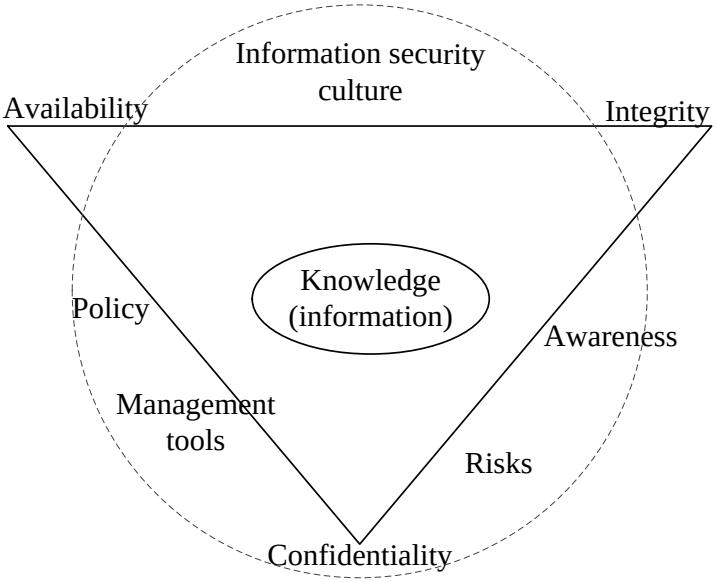

Figure 28: Information security perspectives on knowledge

The information security approach to information and knowledge is to analyse the ideal characteristics of information and, on the basis of the risks to them identified, choose appropriate protection mechanisms. The characteristics for information are viewed as static, or at least the aim with the protection mechanisms is to keep them static (maintain availability, prevent loss of integrity, and keep the information confidential). While the information security management process is described as iterative, the aim of the process too is considered a static goal: a secure state for information.

When the perspectives on knowledge depicted in the various figures are mapped alongside each other (see Figure 29), the differences between approaches are rendered more visible. The process-orientation and dynamism of knowledge management is contrasted with the more static approach of information security management. Although, in the eyes of the author, the management tools and characteristics for information as described in the field of information security do not emphasise the dynamics of a changing environment and increasing amount of information, a dynamic essence is assumed to be present in the reality of information security management.

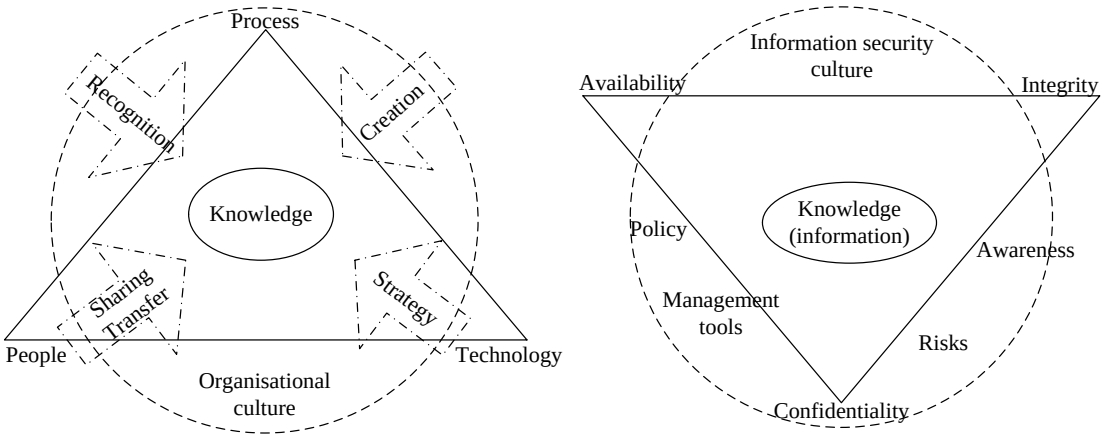

Figure 29: Theoretical perspectives on knowledge

The term ‘culture’ emerges in both of the main fields of theory forming the background for this work with reference to a key driver that affects the success of KM initiatives or information security management efforts. Cultural factors are discussed a great deal in both bodies of literature. One way to success in both of these fields is to create a beneficial organisational culture that supports the activity, whether it be knowledge management or information security. As Figure 29 illustrates, organisational culture is one area in which the ‘powers’ of knowledge management and information security management could be united.

From the figure, the perspectives of knowledge management can be described as involving processes. Knowledge is created, recognised, codified, and shared, for example. The process nature of knowledge management is evident in most of the literature, with emphasis on the dynamic nature of knowledge. Knowledge is constantly subject to many processes of transformation and transfer. A dynamic phenomenon is difficult to tackle with static terms.

In the information security literature, perspectives on information, and on knowledge as part of it, are more static, as can be seen from Figure 29. Knowledge has characteristics that need to be guaranteed. The elements of confidentiality, integrity, and availability are not entirely static, but the idea of a characteristic that can be secured implies that it is static enough to be maintained. There are also policies in place to direct information security activities. The information security policy is defined as a fairly stable document that changes slowly over time. Awareness and culture too are mentioned more as static phenomena, not so much in terms of processes. The process perspective can be seen in the information security literature – for example, in the management models – but it is not as powerful as in the knowledge management literature.

Potential for synergy exists in bringing together the perspectives of knowledge management and information security management on knowledge. The knowledge management perspective brings a stronger dynamic process angle into the picture, and

the information security management perspective contributes utilisation of more static tools. Through a combination of the two, an analytical, process-oriented perspective on knowledge security can be created. This combination of approaches is continued in Chapter 4 of the study, with a systematic literature review addressing both fields of theory from the perspective of the concept of knowledge security. Before that, however, the general approach that small companies adopt toward information security management is examined, for a better sense of what kinds of issues are not addressed in companies and, through this, of the sorts of issues that should be looked into in more detail in the conceptual analysis of knowledge security. The synthesis of the two bodies of theory offers potential for a contribution to work on this concept for companies.

3 The introductory empirical study

The introductory empirical study is presented to provide an overview of the management-related information security issues that companies face. Of special interest is what kind of information the companies consider important and protect through their security activities. The introductory empirical material was gathered in interviews that were conducted as applied information security management assessments. The themes covered in the interviews ranged broadly from security management to technical implementation. In this study, the managerial themes of the material are analysed.

The introductory empirical material is used in this study to deepen understanding of the research phenomenon (see Phase 2 in Figure 8, on p. 15) and of companies' attitude toward important information. It does not directly consider the concept of knowledge security, which is the focus of analysis in this study. Nonetheless, the material sheds light on what kinds of information the companies represented in the interviews considered important and how they were organising their information security activities. This information is of use in considering the concept of knowledge security from the standpoint of organising security activities and recognising important knowledge.

3.1 The research setting

In this section of the thesis, the interview arrangements, interview questions, and analysis method are presented and discussed. The interviews were conducted with representatives of small companies in the Tampere region in spring 2009. The material was collected by university students enrolled in a course on information security management under the supervision of the author of this study. The course setting dictated the size and location of the participating companies. The interview questions were predetermined but somewhat flexible; i.e., the interviews were semi-structured (Fontana & Frey 2005). The interview material was transcribed and analysed in line with content analysis principles. The qualitative research tool ATLAS.ti was used in the analysis process.

3.1.1 Interview arrangements

Eleven small companies in the Tampere region participated in the interviews, in spring 2009. The size of the companies ranged from 7 to 40 employees. Two of the participating companies were independent units of a larger corporation. In their case, the assessment interview covered some corporation-level instructions but concentrated on the unit-level analysis. This is why the size of the unit is reported in all cases as the size of the company. The size range of the companies is reported in Table 3. The companies needed to be small enough for the student groups to be able to compass within one interview. The yearly assessment was offered over the years also to bigger

companies, but the assessment proved most useful for small and middle-sized companies that do not have many resources to allocate to information security. In addition, bigger companies have been reluctant to participate in such interviews and thereby reveal confidential details of their information security to outsiders. In consequence, the participating companies represent a convenience sample in terms of both location and size.

All companies contacted as potential participants in the assessment were small. Uniformity of size would provide a coherent group of companies from the same region and facilitate comparison between companies, which was one goal for the assessments. The companies selected are all in information- or knowledge-intensive industries, so information security has a fundamental role in their operations. Companies that were the right size, suited the purpose of the work, and were accessible were chosen for study.

Table 3: The sizes of the companies involved in the introductory interviews

Number of employees	Number of companies
under 10	2
10–19	4
20–29	2
30–40	3

One or two representatives of each company were interviewed. The interviewee's position in the company ranged from the CEO to information manager and support staff. The companies had been asked to nominate people who were responsible for information security management as interviewees. The positions of the interviewees are listed in Table 4.

Table 4: The interviewees in the introductory interviews

Company	Interviewees
C1	H1: Managing director H2: Project manager
C2	H1: CEO
C3	H1: CEO H2: Financial director
C4	H1: ICT expert
C5	H1: Technology manager H2: Software designer
C6	H1: Unit manager H2: System administrator
C7	H1: CEO H2: Quality manager
C8	H1: CTO
C9	H1: CEO

C10	H1: Vice-CEO H2: Marketing manager
C11	H1: Network expert H2: System administrator

The list of roles in Table 4 attests to a technical orientation to information security. The companies assigned the interviews to people responsible for the information systems they used and were also prepared to provide many technical details on information system security. The companies adopted this approach regardless of the fact that they were told that the interview is not a technical audit. The assessment was introduced as an overview of the organisational information security of the company, one that also considers some technical issues.

The interviews were conducted in spring 2009. The author of this study was present at all interviews, to ensure that all of the relevant themes were covered and that the interview material was coherent across companies. The interviews were conducted by university students under the author's supervision. The interviews were also recorded and transcribed; transcripts enable deeper analysis of the words the interviewees used and how they addressed the issues raised by the interview questions. The interviewees were given the interview questions beforehand for preparation if they asked for them.

3.1.2 The interview questions

The interview questions were grouped under six general themes. The questions of interest for purposes of the present study have to do with important knowledge and motivation for implementing security policy or other security measures. In other words, they were questions about organisational security and personnel security. These questions, listed in Table 5, form part of a 38-question set used in the assessments. The original questions (in Finnish) are presented in Appendix 1.

Table 5: Interview questions in the preliminary study

Question number	Question
4	What does information security mean to the company?
5	What kind of information is there in the company? What information is considered the most important?
9	Describe the information security policy of the company (goals, scope, and whether it is documented). Are there other documents connected with information security (password policy, recruitment policy, general work policy, etc.)? When and why were the policies created, and by whom?
10	How are the information security roles and responsibilities distributed among work roles? How are the responsibilities communicated to employees? When are the responsibilities updated?
11	Are any internal information security assessments performed at the company? How often? Who performs the assessments, and how are they carried out?

12	Does the company monitor information security policy compliance? How?
13	Does the company cultivate employees' awareness of information security (in terms of attitudes and motivation for information security)? How?
14	How are the personnel trained with respect to information security issues? Are there any standard instructions or training materials for new employees? If the personnel are not trained in addressing information security issues, what are the most important reasons for this?
15	Does the company perform background checks of the people it is recruiting? How are the checks done? What kinds of risks does the company see in recruiting?
18	Are there documented or standardised procedures applied when an employment contract ends or is otherwise terminated?

The questions are quite detailed but were not necessarily posed in this precise form to the interviewees. The multiple-part questions were formulated so as to help the students who performed the assessments to understand what kinds of questions could be used to lead the discussion a bit more deeply into each topic. Not all interviewees chose to answer all questions in equal depth, but the material still provides enough information for drawing some general conclusions about the situation at small companies.

The interviews included questions about technical information security also. The main finding on the technical topics is that even small companies need to have technical security covered well. To be able to do business in a networked manner, the companies are required to address many technical security threats regardless of the size of the company. However, talk of the more management-oriented topics elicited more varied and interesting material from the interviews.

The interviews were connected with a university course supervised by the author of this work and were carried out by undergraduates and master's students participating in the Information Security Management course. The students were supervised by the author and prepared for the interviews by going over the interview questions in class beforehand. The students were also expected to analyse the questions and to alter them slightly if the questions were not entirely suitable for the company in question. This preparation ensured that the students performing the interviews had thought in advance about how they would report on the interviews and why they were asking the questions they were given to use.

3.1.3 The analysis method

The analysis method used in this study is content analysis. According to Weber (1990), content analysis can be used for many distinct purposes with qualitative material. One of these purposes is to reveal the focus of individual-level, group, institutional, or societal attention (Weber 1990). In this study, it is employed to find the attitude and

focus of attention of companies with respect to information and information security. This purpose justifies the use of content analysis methods well.

The aim of content analysis is to classify each of the many, many words in qualitative data into one of a few content categories carrying similar meanings (Weber 1990). This means that the analysis method is used to condense the rich qualitative data into a small enough number of textual categories that the richness of the material's qualitative nature is maintained while the dataset is easier to grasp and understand. As Weber (1990) states in his book, 'there is no right way to do content analysis'. This means that the researcher must choose the actual practical steps of how to perform the analysis on the basis of the material that is analysed and the research questions that are to be answered (Weber 1990, Robson 1993 in Elo & Kyngäs 2008).

For analysis of the interview findings, the interviewees' answers were thoroughly read several times. After this initial immersion in the research material began the content analysis process proper. This line of action is suggested in content analysis guidebooks (e.g., Weber 1990), even if their instructions on the latter steps are not as detailed (Weber 1990, Guthrie et al. 2004, Elo & Kyngäs 2008). Although the aim of content analysis is to condense text into more manageable categories, this cannot be done without thorough knowledge of the data. After immersion in the data, the unit of analysis can be chosen on the basis of what kinds of possibilities the data provide in the eyes of the researcher (Weber 1990). The unit of analysis can be lengthy passages of text, sentences, words, or even characters, depending on the research questions (Elo & Kyngäs 2008).

The semi-structured interviews provided 159 pages of transcribed material for analysis. Analysing this amount of text manually would have been a daunting task, so the aid of analysis tools was sought. The interview material was processed into categories with the assistance of qualitative analysis application ATLAS.ti. The software enabled easy access to all quotes of a certain category and aided in determining whether the categorisations are valid. In the course of the analysis, some categories were divided into sub-categories while other categories were merged. The set of categories was in part chosen by the author in advance and partly emerged from the coded material. In this respect, both inductive and deductive approaches (Elo & Kyngäs 2008) to content analysis were used.

Deductive, or structured, content analysis is an approach wherein predetermined categories are used in sorting of the material (Jauch et al. 1980, Guthrie et al. 2004, Hsieh & Shannon 2005, Elo & Kyngäs 2008). The categories are determined in light of theory, and a structured analysis matrix is prepared for categorisation of the text (Jauch et al. 1980). This deductive approach is used mainly for hypothesis-testing or correspondence analysis, comparison to earlier studies (Elo & Kyngäs 2008). The

approach works also, for example, for calculating the frequency of certain words in text and thereby interpreting their importance for the individual or organisation using them (Guthrie et al. 2004, Hsieh & Shannon 2005).

Inductive, or conventional, content analysis, on the other hand, emphasises that the categorisation is generated as the analysis progresses: the categories emerge from common coding of the material via grouping of similar codes together (Hsieh & Shannon 2005). The process continues to further abstraction of the categories, and a model, conceptual system, or group of categories is created as output (Elo & Kyngäs 2008).

The process of analysis in the introductory part of the study was closer to inductive analysis. Though some of the categories were determined on the basis of the theoretical discussion presented in Chapter 2 of this study, no actual analysis matrix was used. For example, text was coded into the predetermined categories of 'important information' and 'information security policy'. As the process continued, other codes emerged as well. Also, the criteria on the basis of which a certain piece of text was assigned a certain code evolved in tandem with the process, leading to recoding. Another factor that supports defining this content analysis process as inductive rather than deductive is the unit of analysis. The deductive approach seems well suited to the analysis of words, but in this case the unit of analysis is a sentence or collection of sentences, a quote or other short excerpt.

Content analysis as a method has received criticism for the ambiguity of the process and the large role of interpretations by the researcher in the analysis (Jauch et al. 1980, Elo & Kyngäs 2008). Another cause for concern can emerge if only one person conducts the analysis (Weber 1990, Elo & Kyngäs 2008). This study displays both of these weaknesses. The weakness associated with the interpretation process of the author having a large role in the categorisations of the data is addressed by means of the use of excerpts (Elo & Kyngäs 2008) to illustrate how the categories have been constructed from the original data. The categories and their definitions are also presented, at the beginning of the discussion of each major topic. This summary of the categories is provided to help the reader understand the individual sub-categories while reading their further descriptions.

In the following discussion, all sub-categorisation is presented in a table, with the categories, summaries of their definitions, and the instances in which these categories are present in the interview material. The ambiguity of the interview material is clear from the fact that a given interview could be placed in multiple categories, and the total sum of instances could, therefore, be larger than that of the companies. For example, in the case of definitions of information security, an interviewee might first give

information security a very narrow definition but later discuss the topic with a broader definition. Such instances are categorised as involving separate definitions.

3.2 Findings from the interviews

In the discussion below, extracts from the interviews are used as illustrations of how the interviewees discussed the topics and answered the questions they were asked. Not all of the answers to each question are presented. Instead, the answers have been categorised by theme, and one or two excerpts per theme are presented as examples of the category in question. Each interview extract begins with a boldface **C** and a number, representing the company the quote comes from. The extracts presented may include statements from more than one interviewee, in which case the speaker is indicated with the interviewee indicators H1 and H2. The roles of each interviewee in each company are listed in Table 4.

> ***C3*** *H2: It is difficult to define what belongs to information security, but if I look at it from my point of view, all information that goes through me belongs to it.*
> *I: There is no completely public information…*
> *H2: Only our advertisements are completely public.*

The example interview extract above is from discussion in the interview at company 3. Here, the discussion is between the interviewer and company representative H2. 'I' refers to the interviewer. While there were up to five interviewers at an interview in the introductory material – since the student group could have four members and the author of this study was present also, sometimes asking the interviewees questions – distinguishing between interviewers was not considered essential to the analysis.

3.2.1 Definitions of information security

The interviewees found defining information security to be a challenging task. The discussion about information security seemed to assume that everyone knows the content of the concept, but explicitly stating what is meant by information security was difficult. Some of the interviewees had clearly prepared for the interview by finding publicly available teaching materials about the topic and therefore answered the question with a definition used in the class taught by the author. This preparation shows that the task of explicitly defining an abstract concept such as information security is by no means an easy one. The answers were categorised by definition of information security; the categories are listed in Table 6.

Table 6: Definitions for information security

Category of the definition of information security	The definition	Instances
Information security is about ensuring confidentiality of information	Information security activities deal with mainly the goal of keeping information out of the eyes of people who are not authorised to access it, either mainly in technical terms or in a broader sense	6
Information security is an all-encompassing activity	Information security includes the confidentiality, integrity, and availability of all information the company handles, and employees' behaviour has a large role in this	6
Information security is a technical issue	Information security means information stored in information systems being protected by technical means against viruses, hackers, and equipment failure	3

Many interviewees approach information security from the point of view of *confidentiality*: if information is classified as confidential, it falls under the umbrella of information security. These interviewees brought many technical aspects into the definition of information security, focusing on how to keep the information in information systems confidential and not leak it outside the company. Confidentiality, according to the interviewees, means that information that is meant to remain inside the company stays there.

> ***C2*** *H1: Information security means that information that belongs inside the company does not end up outside the company. This includes especially the information that belongs to our customers too.*

> ***C3*** *H2: It is difficult to define what belongs to information security, but if I look at it from my point of view, all information that goes through me belongs to it.*
> *I: There is no completely public information…*
> *H2: Only our advertisements are completely public.*

These quotes represent the confidentiality-based category of definitions for information security. With this category, information security is seen as an activity that ensures the confidentiality of information. Confidential information is considered important, and it should be protected against leaking outside the company.

In addition to the confidentiality discussion, other dimensions to information security are found in the answers. Six companies acknowledged that information security is more than mere technological solutions to ensure the confidentiality of information.

They brought up the other characteristics for information mentioned above, availability and integrity. What these terms mean for the company, however, is not found in the answers; they are only mentioned as terms that were familiar to the interviewees either from daily use or from familiarisation with the terminology used in lecture materials.

> ***C11*** *H1: The information that we want to keep secret and inside the company; we do our best to keep it that way.*
> *H2: Of course, there is, of course, more to it, actually all the material that we use.*
> *H1: We try to minimise leaks. And, overall, any [threats] that we can foresee. Maximising safe use of information.*
> *H2: Then there, of course, is integrity and availability of information and all that. It's quite difficult to articulate what [information security] actually means.*

This excerpt represents the category of definition of information security as an all-encompassing activity. Confidentiality is still mentioned as the most important characteristic, but the other characteristics are acknowledged. In addition to the characteristics of secure information, this company (C11) mentioned safe use of information: information security, according to them, is about minimising information leaks and maximising safe use of information. They acknowledged that it is difficult to explain all that information security encompasses, but the answer elucidates that there is more to it than just the safe use of information systems.

Other companies made tentative expansions of the narrow definitions of information security by addressing the behaviour of their employees. However, this kind of definition too emphasises the use of information systems and appliances in various environments as examples of the behaviour.

> ***C1*** *H1: It is all-encompassing behaviour. Of course, these [discussions about information security] emphasise IT and […]. Material like that, the behaviour of people, is part of the technology. I mean how they behave at customer offices, [and] on buses, and [whether] they have locked their mobile phones and such.*

Some of the companies that defined information security to be an all-encompassing activity also emphasised that information security is based on the behaviour and activities of people. The examples of behaviour given are related mainly to the use of information systems. Two of the examples the interviewee at company 1 gave differ from system examples. He pointed out that how people behave on customer premises and while they are travelling is a big part of information security. The context of this answer implies that these examples have to do with how people use their information appliances in these environments, but the interviewee may have had a broader perspective in mind.

The difficulty of defining what information security actually is is an interesting finding. It points to information security as being a matter that people take for granted, trusting that the concept is implicitly understood by everyone. The interviewees had, after all, agreed to be interviewed about information security, and that leads one to assume that they had a clear opinion or understanding as to what information security is. The difficulty of articulating a definition and the variety of answers to the question, however, highlight the concept of information security as not implicitly clear to everyone, at least not in a uniform way.

Many of the interviewees did not mention the availability and integrity of information as important aspects of information security. This might be because the solutions for technical availability and integrity, such as backup routines, mirrored servers, and anti-virus protection, are clear necessities to companies. They may not even be considered to involve information security activities. Instead, they are considered vital elements of daily action. However, availability and integrity extend from technical elements to encompass information and knowledge that is not stored in information systems. Furthermore, even in information systems, the integrity of information requires more attention than just backups – for example, in the form of mechanisms to ensure that accurate information is fed in to the system. Integrity and availability of knowledge are even more difficult to address. The introductory material indicates that these were not considered information security issues by many interviewees.

3.2.2 Important information

In addition to how the interviewees actually defined the term 'information security', what information they considered important for their company says something about their approach to information security. The question about important information was posed to reveal whether the companies had thought about what information they need to protect and also prioritised among distinct kinds of information. Recognising which is the important information is one step toward managing and protecting that information, as was discussed in the theoretical material in the previous chapter. The categorisation of what information the interviewees considered important is summarised in Table 7.

Table 7: What was deemed to constitute important information

Category of the definition of important information	The definition	Instances
Customers' information is the most important	All information that belongs to the customers or is related to the customer relationship is most important and valuable for the company	8
Product information is the most important	The information related to the development of products is the most important for the company	3

All information is important	All information that the company handles is important; it is impossible to prioritise any as more important than other types	2
Knowledge of employees is the most important element	Employees of the company possess knowledge that is vital for the operations of the company	1

The response most commonly given to the question about what information is important for the company is that the customers' information is the most important. This was the category emerging first in the responses, with eight instances in the interviews. When referring to this customer information, the interviewees meant, for example, planning documents, contracts, pricing information, specifications, personal details, and financial data connected to the company's customers. This was considered the most important of the information that needs to be protected against leaks. Leaking information that belongs to customers would lead to loss of trust and very likely to loss of business. All interviewees stated that all employees know this and treat the information accordingly.

> ***C10*** *H1: We have performed some risk analyses and considered what information is important […]. We deal mainly with customer projects, and if we leak our customers' information, we don't lose anything apart from our reputation. So even if it's not critical from our point of view, it is critical to the customer.*

This quote represents the category of response in which customers' information is the important information theme in the interviews. The emphasis expressed in what kind of information the customers provide for the companies depended on the type of business, but all of this information was considered critically important. The company could, in theory, continue to operate normally even if leaking or losing information that belongs to a customer. What makes the customer information critical is that how a company treats information affects that company's reputation among current and prospective customers.

Another type of information cited as important is information on the company's own products. The product varies, depending on the industry of the company, but many of the companies were conducting some product development of their own and considered it important and in need of protection. Interviewees with three of the companies mentioned this information as the most important.

> ***C1*** *H1: Well, it is our own IPR and IPR of customers. And trade secrets, but it is quite-*
> *H2: I think the most critical is the information of our customers. There are possible sanctions if it is leaked.*
> *H1: And otherwise too. It is not the worst scenario that [these things] leak.*

This extract represents the category of in-house product development information under the theme of important information. While recognising the information of the company as important, the interviewees here acknowledged the importance of customers' information, so this excerpt belongs in the customers' information category too. They also led the discussion into the threats that the information faces. The biggest threat may not always be information leaking outside the company. However, the main interviewee here does not elaborate on what he may see as the greater threat to important information. One scenario might involve the information being lost altogether, because of, for example, equipment failure, human error, or a combination of the two.

Intellectual property rights are one angle in description of product information. The IPR – meaning patents, copyrights, etc. – is information that is protected by copyright and other laws: when created by the company or customers thereof, it is the property of the creator. Whilst protecting the IPR of a company is easier when as little information as possible is published, the patenting process makes information public, so many companies choose to eschew it and to focus on just keeping trade secrets.

Leaks of information to external parties are seen as a major threat to important information, but some of the interviewees acknowledged that leaks are not the only threat and are not always even the worst one. Other threats may receive less attention because of the implicit assumption that information security involves ensuring the confidentiality of information. In the extract directly above, interviewee H1 states that information leaking outside the company may not be the greatest threat to C1's information, assumedly referring to the threat of losing the availability or integrity of the information through, for example, broken equipment. Whether the statement below refers to knowledge and departure of employees is unclear, but some interviewees did state outright that the knowledge of employees is important for the company.

> ***C8*** *H1: But what is a big challenge is that our staff have knowledge in their heads. I mean people who leave the company. You cannot build a system to keep that knowledge secure.*

Company 8 has recognised what a great challenge it is to ensure security of information or, more specifically, knowledge that resides in employee heads. This quote falls into the 'knowledge of employees' category under the important information theme. This company feels that security of knowledge is impossible, since 'you cannot build a system for it'. That implies that the interviewee deemed information security mainly about building systems for secure information. This notion is one key trigger for the primary empirical part of the study: can knowledge security be achieved systematically, and, if it can, how is that done? At the same time, do all companies consider security of knowledge impossible?

Overall, the companies have stated, via their representatives in the interviews, that the information belonging to their customers is the most important information and receives the greatest security efforts. This is not surprising, given that the participating companies were small and many of them had a major role as a subcontractor for a bigger company. It is understandable for one in such a position to put a strong emphasis on the information the customer provides. The relationship with the customer may be very close and the information exchanged with the customer very high in volume and strategic in nature. The companies that were not so close to their customers emphasised the importance of customers' information less, which supports this interpretation.

The role of the company's own trade secrets also varied between companies, depending on the type of their business. If there is no in-house product development, there is no such information to protect. In the companies that did have their own product development, the information on it was defined as important and subject to information security activities.

3.2.3 Organisational security

The security management organisation of the companies itself reveals in part the level of emphasis on information security. By assigning information security roles to its personnel, a company makes a statement on how important it considers information security to be. The company also reveals its views of information security through its security management documents. Documenting roles and responsibilities in an information security policy is one way to stress the importance and scope of information security. Table 8 presents a categorisation by the kind of information security documents the companies had.

Table 8: What information security policy was defined as entailing

Characterisation of documentation of information security policy	The definition	Instances
A documented information security policy	The company has an information security policy that corresponds to the definition used in this study	2
Technical security policy	The company has documentation that can be considered to involve technical security policies.	5
No need for information security policy	The company has not established documents that explicitly address information security	4
Emerging need for policy	The company does not have a policy document, but a policy will have to be formed within the next year	1

As Table 8 indicates, two of the companies had a documented information security policy. One of those companies was part of a larger corporation, and the security policy

had been handed down from that higher level. The other company had had a consultant help create an information security policy for them. These two companies were categorised as having a documented information security policy. In addition to these two companies, one company had a quality management system that included a security management strategy bearing many similarities to an information security policy though quite technical and thus narrower in scope. This is why, regardless of the name of the document, this company was placed in the technical information security policy category.

Most of the companies did not have an information security policy document as defined in this study. The topic of information security, however, was addressed to some extent in, for example, work instructions, password policies, technical manuals, internal wikis, and network documentations in some companies. The associated documents can be considered technical information security policies, as they usually instructed in the secure use of information systems or other technical aspects of the work. At these companies, information security was considered mainly a technical issue; in these cases, the technical information security policy category was appropriate.

Some companies had no documentation that could be considered even a technical information security policy. The interviewees at these companies felt that their companies were so small that they do not need a written document to communicate something that they can pass along through simple discussions.

> ***C4*** *H1: No, we don't have much [information security policy] documented in fancy words. We handle it more via discussions. We are quite a small company, after all.*

This quote represents the 'no need for information security policy' category. The main reason cited for not documenting the information security policy is that the company is so small that communication on information security can be handled through discussion. The interviewees indicated that they felt an information security policy would need to be an official and fancy document, which they did not want to have.

> ***C5*** *H2: No, we have it [information security policy] integrated into our common practices […].*
> *H1: And job descriptions and such. We have seen it; we are quite a small company, and a policy document is more a tool for bigger companies. We have the challenge that even if we did create this fine information security policy [and] our management say that this is our vision of information security, it would not really affect anything.*

In this example from the 'no need for information security policy' category, a participant stated that the company do not have an information security policy and prefer not to have one. They felt that it would be a useless level of bureaucracy and that the employees would see the policy not as a tool but as a meaningless document that

does not affect them. Instead, the issues that could be addressed in an information security policy were addressed in job descriptions and instructions, so that they would be expressed as close to the employees' day-to-day work as possible.

The interviewees at C5 felt that an information security policy is a tool for larger companies in need of a coherent way of communicating to larger groups. Many of the participating companies had employees who possessed years of experience in working for large companies. Characteristic of this experience is heavy corporate bureaucracy. The interviewees stated that one major reason people like to work for small companies is the lack of bureaucracy. If the employees see the information security policy as a manifestation of an inflexible, bureaucratic organisation, it is probably wise to communicate the information-security-related goals and responsibilities in a different way.

One company's staff stated that they would need to create an information security policy in the near future. So far, they had had some documents to instruct the employees, but a more structured approach was deemed necessary. Structure was needed in information security documentation especially to communicate responsibilities. Hesitation to document responsibilities was connected to the bureaucracy issue mentioned above.

> ***C1*** *H1: We need to document the information security roles and responsibilities explicitly. We have avoided this in the past because it may lead to people not reacting to things that they see, since doing so is not explicitly their responsibility. But to reach the next level of growth, we need to define some responsibilities to give some structure to our operations. But the downside of responsibility charts is 'this is not my problem'.*

In this example from the category 'emerging need for policy', the interviewees considered the associated division of responsibilities not wholly a good thing. Yet clear documentation of responsibilities was still seen as a necessity, no matter the possible negative results of people not taking action since someone else is officially responsible.

The answer most commonly given when the interviewees were asked about information security responsibilities was that everyone is responsible for his or her own information. The responsibility for information security was specified for all job roles, in line with the associated level of access to information of various types. These answers proceed from the above-mentioned understanding of information security as mainly a technical issue. In this technical view, responsibility for information security is assigned to the people who develop and maintain the technical systems that the company uses.

> ***C8*** *H1: It is the managers of individual functions who define [the responsibilities], and it is their job. And usually it is the CEO who [is*

responsible for] most of the things […] and defines responsibilities. But when it comes to technical information – I mean product development – it is the technology manager (and, in production, the production manager) who sees to it that the necessary information is behind passwords and is accessible only to those who need it.

In this response, the practical orientation of the companies is clearly expressed. The people who deal primarily with information, of various kinds, are responsible for it also in security terms. Perhaps delineating separate information security responsibilities could put too much distance between the practical work and information security efforts. On the other hand, the list of interviewees in Table 4 (on p. 72) tells us something about the distribution of the responsibility for information security. There is a tendency for the people responsible for information security to be those who are responsible for information systems' administration. The CEOs of the smallest of the companies spoke of feeling a personal responsibility for information security but still considered most of the responsibility to have been delegated to the IT administration.

The companies with a documented information security policy had analysed the various roles in information security management in more depth. At these companies, one or two people were responsible for developing the policy and providing training on it. The responsibility for technical security was usually assigned to the IT maintenance staff; the two companies in question had acknowledged that information security is not just a technical concern.

The responses on the matter of responsibilities highlighted a weakness of the data collection method. Different interviewer groups had understood the matter of responsibility differently, and this was evident in how they posed the related questions. Furthermore, the interviewees varied greatly in how they thought about the question of responsibility, thereby making the range of focus of the answers even greater. In analysis of the interviews, it was clear to the author that the answers are not comparable in all respects. Although this weakness exists, in principle, for all of the questions, the topic of responsibility turned out to be the one for which it is most visible in the data.

3.2.4 Information security training

The literature considers information security instructions and policies to be an essential tool for managing information security in companies and training employees. Educating the employees on the contents of the policy and the grounds for it is a way to ensure that employees are aware of the policy (von Solms & von Solms 2004a, Peltier et al. 2005, Crossler & Bélanger 2009, Tsohou et al. 2010). Awareness is the first step toward the policy being followed by the employees. The training offered by the companies was categorised by the type of training offered. This categorisation is summarised in Table 9.

Table 9: Characterisation of information security training

Category of information security training definition	The definition	Instances
Training in introduction	Training in information security is offered upon the arrival of a new employee	7
Designated information security training	The company has offered training to educate its employees about information security issues	1
Information security training as important	The company considers information security training important and plans to arrange training to educate employees about information security issues	1
Notifications and discussions	Information security training is handled through notification of employees on current information security issues and discussion of current topics in weekly meetings	4
No security training	Security training is not offered at all	2

Most of the companies provided new employees with some kind of training upon their arrival at the company. Seven companies included information security in the topics of induction training for a new employee. In most cases, the introductory training included instruction packages to read and, after this, some discussion with the supervisors on the basis of the materials.

Information security training was seen as important by some of the companies, but even if the training is considered important, the reality is that allocating resources – namely, time – to training competes with many more business-critical operations in small companies.

> ***C1*** *H1: We have information security training in the budget. Either we buy it from outside or one of our customers can provide some training for us. But we'll see […]. It's not exactly in the top three priorities […]. [At present] we discuss things and remind about them at weekly meetings.*

This example, from the category of training as important, shows the challenge of prioritisation. At the time of the interviews, the company were holding some discussions considering information security, and they had considered investing in more formal information security training for the employees, but that investment was not going to be made to the detriment of critical business activities. Information security training competes for resources not only with critical business activities but also with other, lower-priority investments.

> ***C4*** *H1: [U]sually it is by discussion and talking. It is… I'd say that it is challenging to arrange it [information security training]. From my experience, not connected to this company – […] I have been in a relatively large defence-sector company – it doesn't matter how much you train people: it doesn't seem to interest them. I don' t know why.*

The interviewees considered traditional lecture-style training challenging. They stated that people do not want to attend training sessions and are unwilling to participate in the training. The reason for this lack of interest, however, was less clear to this interviewee.

In two of the companies, employees did not receive any information security training. One reason for this was that most of the employees were highly educated and experienced technology professionals, so they did not think that the training would provide any value for the company. The companies with more systematic information security training in place did not mention that it would have been challenging or badly received by the employees. The company with a documented information security policy deemed the documentation and training to have been a positive thing:

> ***C10*** *I: [H]as the documentation been worth the effort?*
> *H1: At least I like that we have it [information security policy] on paper now. It is easier to instruct and train [the employees] and say that this is how we do things, instead of just talking about it. We have had only a few changes in staff overall, so we haven't had much need for the documentation, but it is great that we have it here now. I especially like the appendix to the employee handbook, which is very detailed, although I don't know how carefully people read [it]. At least we have gone over everything once, in the training.*

Information security instructions or policies and training seem to support each other, even though no statistical evidence of this is demonstrated in the present work. The more training a company offers, the more structure it needs to its instructions and policy. On the other hand, training is easier to offer when there is a structured set of policies and instructions. The attitude of the management toward training could be a driver for successful training. The interviewees at the companies that offered no training felt that the employees would reject it. On the other hand, those with the companies that did offer some training did not mention any problems with staff attitudes. This observation is only a tentative one, however, since the material is quite limited.

Attitudes toward information security training provide one lens for peeking into the security culture of a company. The attitude toward information security training may reflect the attitude of the managers and employees to information security overall. The general attitude at the companies where no training was considered necessary or desired might be an indication that information security was taken for granted. Another possibility is that information security was considered 'not my job' and, accordingly, not deemed important. In light of the interviews, however, the first of these possibilities,

information security being taken for granted, seems more likely. The interviewees expressed trust that the employees are knowledgeable about information security issues, which is an indicator of overall awareness of information security issues and of according importance to them.

The companies that offered information security training or at least addressed information security issues at their meetings thus show a positive attitude to information security. Information security was considered important at these companies, so time and money were invested in promotion of security activities. This security-promoting attitude reflects an information security culture wherein people's general attitude to information security is positive.

3.3 Summary of the introductory study

The introductory material presented in this chapter shows that the companies taking part in the interviews had addressed the technical issues of information security well, which is a prerequisite for conducting business in a modern networked society. However, the interviews also show that many of the companies considered information security to be associated mainly with technical solutions and mainly for ensuring confidentiality of information. Wider perspectives on the definition of information security were found in the interview material, but the general stance on information security was that it is a technical matter and considers mainly technical solutions for ensuring the confidentiality of information stored in information systems.

The organisation of information security responsibilities evidenced further supports the observation that information security is considered mainly a technical issue, although more aspects to it were recognised by some of the companies. Most documentation of policies and procedures was done in relation to technical information security. The emphasis on technical elements is visible from the interviews, with many examples of information stored or transferred in information systems and much discussion of it.

The technical orientation of information security work at the companies reflects the focus of the operations of the companies: they were mainly in the high-technology industry. However, all of them had knowledge workers and experts working for them, and not all of the associated knowledge could be stored or transferred within the information systems. Some of the companies acknowledged that training the employees and increasing their awareness of information security is essential, but even basic training tended to be placed near the bottom of the prioritisation list. The companies that had acknowledged the need for other than just technical and confidentiality-based information security considered it to pose a true challenge for them.

When drawing forth further observations from the introductory empirical study, one must keep in mind that the interviews were conducted to assess the overall information

security status of the companies and that the interviews did not focus on knowledge. However, the interviews were conducted in Finnish and the concept used was *tieto*, which encompasses data, information, and knowledge. Therefore, the discussion could have covered knowledge also in a larger extent if the interviewees had felt that it belongs to the scope of their information security activities. Also, the interviews' emphasis on the managerial and organisational component of information security left a large amount of room for discussion of knowledge, again if the interviewees considered it a relevant issue falling under the general topic.

The analysis of the introductory material points to a need for the concept of knowledge security and justifies it. At least in small companies, information security is considered to be mainly a technical issue. It is also approached primarily from the confidentiality angle. The concept of knowledge security could broaden the scope of security activities, extending it beyond the boundaries of information systems. It could also elevate the role of the other characteristics – availability and integrity – in the security discussion. These characteristics are all equally important, both within and outside the technical systems. Some of the interviews described in the introductory material underscore the need for knowledge security, even though – and, in a sense, precisely because – it was considered very difficult by the interviewees. This study was, after all, triggered by the author's curiosity about this phenomenon that some interviewees disregarded and others acknowledged but found very tricky to approach. Careful analysis of the concept could give a name and definition to the concept, thereby rendering it manageable. The difficulty of tackling knowledge security should not be deemed reason for not considering it.

However, the concept of knowledge security itself does face challenges. Securing knowledge in companies should not require additional effort and separate investments of time, money, or both. If knowledge security can be achieved in a manner that benefits the company in other areas too, it may be very attractive. This is why the connection between the fields of knowledge management and information security should be examined more deeply. Knowledge security may well be the concept that brings the benefits of knowledge management and security efforts together and, in so doing, makes the efforts in both more attractive. Especially in small companies, 'killing two [or more] birds with one stone' is a highly attractive option.

4 Knowledge security

The previous chapters have introduced the theoretical background for this study, and Chapter 3 presented an empirical introductory study that sheds practical light on the theoretical background. From the introductory study it is evident that companies struggle with the theme of knowledge security, although this is not a topic of active discussion and problem-solving. Therefore, further examination of the concept is needed. Since the concept is young and not widely used, a large amount of emphasis is given also to parallel concepts. This chapter proceeds toward a theoretical definition for the concept of knowledge security.

This chapter reports partly on phases 3–6 of the conceptual analysis process as illustrated in Figure 7 (see p. 14). First, the various interpretations and uses of the concept are explored (step 3, Section 4.1) along with the parallel concepts (step 4, sections 4.1 and 4.2); then, initial characteristics of the concept are identified (step 5). Finally a theoretical model and definition for the concept are generated (step 6, in Section 4.3).

The introductory chapter mentioned that the literature does not always use the term ‘knowledge’ when referring to the concept of knowledge. The analysis in Section 4.1 concentrates on the uses of the actual term ‘knowledge security’ and its parallel expressions that use the term ‘knowledge’. Section 4.2 complements this analysis by including other terms that may be used to carry a meaning similar to that of ‘knowledge security’. The parallel terms addressed in Section 4.2 do not necessarily feature the word ‘knowledge’; instead, the interest is in the meaning ascribed to terms and concepts, while the focus in Section 4.1 is specifically on the use of the word ‘knowledge’.

4.1 Use of the term ‘knowledge security’ in the literature

For this section, a systematic literature review was conducted for determination of where and how the term ‘knowledge security’ is used. This exploration covers step 3 of the theoretical conceptual analysis illustrated in Figure 7, on page 14. According to Tranfield et al. (2003), systematic literature review is a methodology more commonly used in disciplines that emphasise quantitative research. In those disciplines, a systematic review serves as a basis for formulation of quantitative empirical studies. A systematic review is called for also in qualitative research, to ensure that all relevant research is taken into consideration. Especially in management research, the literature reviews tend to be implicit, guided by the opinion and intuition of the researcher. (Tranfield et al. 2003) With a systematic approach, the role of the researcher is made more explicit, and the significance of intuition is reduced through specification of explicit, reasoned criteria for an item’s inclusion in the review.

Tranfield et al. (2003) introduce the stages of a systematic review composed of three larger parts: planning, conducting, and reporting on the review. This set of stages has been applied in the present study in a modified way, an application presented in Table 10.

Table 10: The stages of a systematic review (modified from Tranfield et al. 2003, p. 214)

Stage I: Planning of the review	**Implementation in this study**
Identification of the need for a review	The review of knowledge security was needed for determination of all possible uses of this concept
Preparation of a proposal for a review	A proposal was formed in the research plan for this study
Development of a review protocol	The keywords for the searches and criteria for inclusion were chosen
Stage II: Conducting of the review	**Implementation in this study**
Identification of research	In this case, the fields of study were identified and top journals from these fields selected
Selection of studies	All papers that mentioned knowledge security, or came close to the concept, were selected
Stage III: Reporting and dissemination	**Implementation in this study**
The report and recommendations	The review was reported upon in line with the plan; no detailed comparison of the papers or of their methodologies was done

For the planning phase, Tranfield et al. (2003) suggest that a review panel be formed and that the protocol be followed by multiple persons, to avoid bias in the use of selection criteria. Since this study was not part of any research project that would have had multiple persons working on it, the review has been conducted only by the author, and the review panel was effectively formed by the supervisors of the study. The method of systematic review was selected so as to introduce as much rigour to the process as possible and to establish a method of reporting that could set out the results of the review in a structured way. In the reporting, a concept matrix approach suggested by Webster and Watson (2002) is utilised to clarify the findings.

4.1.1 **Top-journal review**

The review was performed in three stages. First, 12 journals were selected for systematic review to uncover what the top journals on information systems, knowledge management, and information security are publishing in the area of knowledge security. The systematic review entailed going through 10 volumes of the journals.

The first stage of the review provided the researcher with insight into the current research themes. It also confirmed that the theme of knowledge security is not visible in

the top journals of the core research fields considered. The journal volumes were screened on the basis of title and keywords, and the articles that seemed connected somehow to the theme of knowledge security were further examined on the basis of the abstract, with the most promising ones read in full. This stage aided in the writing of Chapter 2, but it also confirmed to the author of this study that the concept of knowledge security is used little in the top publication venues of the two theoretical fields examined, since it is an emerging topic.

This section of the dissertation presents the results of the systematic journal review. The review was performed manually and involved going through all of the titles and keywords of the articles in the journals selected. Some of the abstracts, chosen on the basis of the titles, were read, and some of the articles were chosen for a full reading on the basis of the abstracts. The reason for selection of the last 10 years for review is that this time span is long enough to show the variety of discussions that have taken place in the journals. Since knowledge security is an emerging concept, a decade is likely to be a long enough time to include most instances of use of the term.

Information systems journals

The top five journals in the information systems field were chosen from the AIS 'Senior Scholars' basket of journals. This set of eight journals represents the top journals in the field from a long-term perspective. Since the AIS journal ranking changes every year, the association has provided a selection of prestigious journals that may change positions in dynamic rankings but nevertheless remain in the top band of the ranking list. The information systems journals reviewed are these:

- *MIS Quarterly* (MISQ)
- *Information Systems Research* (ISR)
- *Journal of Management Information Systems* (JMIS)
- *European Journal of Information Systems* (EJIS)
- *Information Systems Journal* (ISJ)

The five journals selected for review from the eight-journal basket were chosen on the basis of relevance to the topic of this study and availability of full text to the researcher. The most recent 11 volumes of these journals (for 2002–2012) were searched systematically for relevant pieces, first on the basis of title and keywords and in the second phase in view of the abstract. If the abstract held promise of the article perhaps touching on the topic of knowledge security, the full paper was read. In the information systems journals, a promising piece might, for example, be one referring to the use of knowledge management theories or featuring the word 'security', 'information', or 'knowledge' in its keyword list. The search results are summarised in Table 11.

Table 11: Summary of the review of information systems journals

Journal	Articles	Knowledge	Security	Knowledge security	'Close calls'
MISQ	430	29	8	0	0
ISR	322	12	11	0	1
JMIS	459	34	10	0	0
EJIS	506	23	9	0	0
ISJ	273	14	3	0	0
Total	1,990	112	41	0	1

In Table 11, the columns are composed of author-provided keywords. Although all articles were manually checked, the best way to determine whether an article pertains to a topic or not seems to be to look at the keywords the author provided. In consequence, an article is listed in the 'Knowledge' column if the word 'knowledge' is present in the keywords. In the majority of the articles, the actual term used was 'knowledge management', but 'knowledge systems', 'knowledge work', and some other terms were used also. This is why the word 'knowledge' was used as a search item: it encompasses all of these variations. The numbers in Table 11 show that there is discussion of knowledge and security in the top information systems journals. However, these perspectives do not overlap. Also, the numbers show that both of these discussions have a rather marginal role in the journals relative to the total number of articles.

The result of this search of the information systems journals was not surprising: no articles were found that would be directly connected to the topic of knowledge security. Some of the articles considered knowledge, but from the information systems point of view. This means that knowledge is considered an object that can exist outside an individual; that is, knowledge is codifiable (Schultze & Leidner 2002). Furthermore, codifiability leads to improvements in efficiency via the use of knowledge management systems (Poston & Speier 2005, Ko & Dennis 2011). Not all of the articles, however, consider knowledge a codifiable asset; many acknowledge that there are difficulties in capturing the knowledge of experts in knowledge systems (Chiravuri et al. 2011, Durcikova et al. 2011). Some authors assert that knowledge cannot be captured at all in systems, that instead the systems can be used to facilitate person-to-person communication (Lindgren et al. 2003).

The security perspective proved not as commonplace as a knowledge-management-based approach to information systems was. This might be because many security-related articles are technically oriented (e.g., Mookerjee et al. 2011, Chiravuri et al. 2011) and the more technically oriented journals are, therefore, a more natural publication venue for them. Some security-related articles were found nonetheless. When not technically oriented, they discussed, for example, the role of the employees as users of information systems and followers of information security policies (Boss et al. 2009, D'Arcy et al. 2009, Herath & Rao 2009, Myyry et al. 2009, Guo et al. 2011), or the financial considerations surrounding information security investments (Wang et al. 2008). The articles present one cause of threats to information security as being the people who use

the systems. This discussion takes a step toward the concept of knowledge security; however, the perspective of these articles is still that of the security of information stored in the information systems. The role of people as a knowledge repository or a threat to *knowledge* is not visible. Verging on knowledge security (a 'close call') is some discussion of ambivalence in knowledge sharing and protection in online communities (Jarvenpaa & Majchrzak 2010). In the relevant article, the people and their knowledge are considered valuable and worth protecting, although the viewpoint is not entirely that of security.

In summary, the systematic review of information systems journals showed that, whilst knowledge management is an issue that is discussed in information systems journals, the approaches focusing on security and on knowledge were not combined in any of the articles reviewed. The paper coming closest was one that combined discussion of the themes of knowledge sharing and protection. Although it does not use the term 'knowledge security', it is related to the concept.

Knowledge management journals

Knowledge management is a relatively new area of research, so KM journals are not listed in those rankings of the most prestigious journals that are based on impact factors. However, there has been some interest in which are the most important publication venues in this field. Bontis and Serenko (2009) have gone to the effort of devising a rating scheme for KM journals. with KM scientific contributors assigning scores. The KM journals selected are at their levels A+, A, and B. These KM journals were chosen:

- *Journal of Knowledge Management* (JKM)
- *Journal of Intellectual Capital* (JIC)
- *The Learning Organization* (LO)
- *Knowledge and Process Management* (KPM)
- *Knowledge Management Research and Practice* (KMRP)

The journals listed are the five journals highest in the ranking by Bontis and Serenko (2009). These journals too were systematically searched, over the last 11 volumes. The systematic review in the case of the KM journals consisted of looking for any kind of security perspective on knowledge. This meant searching the articles for topics such as trust, risk, protection, and security. A summary of the review is presented in Table 12.

Table 12: Summary of the review of knowledge management journals

Journal	Articles	Security	Risk	Protection	Trust	Knowledge security
JKM	649	1	4	85	10	3
JIC	370	0	2	0	3	0
LO	367	0	3	0	6	0
KPM	253	1	0	0	1	0
KMRP	331	0	5	0	13	0
Total	1,970	2	14	85	33	3

The topic of trust is quite visible both in the knowledge management literature and in the information systems literature. For example, half of the *Journal of Knowledge Management* articles found were listed under the search 'trust', although only 10 list this in their keywords. However, the approaches to the topic differ, depending on the main focus of the research. In day-to-day life, trust is connected to one's sense of security: I feel secure if I can trust the person I am dealing with. In the literature, trust is examined from the perspective of how to establish it between individuals within the organisation (Holste & Fields 2010, Zhang & Sundaresan 2010), between an external party and an individual (Ko 2010), or between organisations (Niu 2010). In the knowledge management domain, trust is examined in terms of how to get actors to trust each other so that they can effectively share knowledge with one another. Trust in this case means people trusting that they will somehow benefit from sharing and receiving knowledge. A security perspective on trust would turn this setting around: Whom can I trust, and what harm can result from trusting the wrong party? This security perspective on trust is not found in the knowledge management literature.

The term 'risk' is present in many articles. For the most part, it is used in connection with financial terms, in which context it refers to potential for financial loss. At the level of keywords, the term 'risk' is not so commonplace in the knowledge management literature. There are only a few articles that identify 'risk' as a keyword. In these articles, knowledge management is seen as a way of diminishing risks, for example, by documenting knowledge that would otherwise be lost through employee turnover (Neef 2005). Another article discusses the need for managing knowledge about risks in addition to managing critical business knowledge (Massingham 2010).

'Protection' is found as a term used in some of the articles, one for which 85 search results were found from the *Journal of Knowledge Management*. Most of these articles (n = 38) use the word 'protection' in a context apart from the term 'knowledge protection'. The latter term is used mostly (n = 18) in connection with intellectual property rights, such as patents and copyright. These rights need to be protected, since the IPR can be a major capital asset for companies (Sanyal 2004, Chou & Passerini 2009) (the focus of this study is not, however, on the legal aspects of IPR protection, since the knowledge connected with IPR needs to be carefully documented in explicit

form so falls predominantly beyond the scope of interest for this study as shown in Figure 11, on p. 28). Several articles (n = 15) mention knowledge protection as one part of knowledge management; however, these pieces do not elaborate on what the term means. They limit their attention to examination of other aspects of knowledge management. Another perspective from which knowledge protection is mentioned (n = 5) is that of the protection of personal knowledge from colleagues (e.g., Ford & Staples 2010, Husted et al. 2012), protection of personal knowledge being considered one barrier to efficient knowledge sharing in organisations. Finally, some articles (n = 9) do address knowledge protection in a way that is interesting from the point of view of this dissertation. These articles discuss knowledge retention, protection of knowledge in strategic alliances, and knowledge protection as an element of knowledge management strategy. Through this discovery, one can situate the concept of knowledge protection as a potential parallel concept to knowledge security. The articles addressing this topic are discussed further in Section 4.2.

The word 'security' is present in some articles but is not given a role that would connect it directly with knowledge. The articles mentioned above were all connected also to the word 'security' in some fashion, although this was not visible from the keywords. The knowledge management journals published some articles that are related to the term 'knowledge security'. The term itself is present in three of the articles, as can be seen from Table 12, but with different meanings. One refers to the technical way of keeping 'knowledge' secure between systems (Chi & Holsapple 2005) – i.e., the decision on what information is to be shared between systems at the level of automatic communication. Another meaning – also a technical one – connects it with systems for security of both information and knowledge (Ergazakis et al. 2006). The third perspective on the term is that of use of knowledge management systems as a way to secure knowledge for future use (Randeree 2006); in these pieces, knowledge is considered a codifiable asset and an element that can be retained in documents.

Information security journals

The two journals that were selected to complement the set of journals in the systematic review described above are the top two journals in the area of information security management. These journals are the two main publication fora for scholars in the field of information security management. These journals were chosen to be examined:

- *Computers & Security* (C&S)
- *Information Management & Computer Security* (IM&CS)

Since these journals publish research into information security management, it was assumed that some papers in them might show a direct relationship to knowledge security, perhaps even featuring that concept itself. Since the journals' field is information security, the key term that should reveal discussion of knowledge security is 'knowledge'. A summary of the review is presented in Table 13.

Table 13: Summary of the review of information security journals

Journal	Articles	Knowledge	Knowledge security
C&S	973	0	0
IM&CS	596	11	0
Total	1,569	11	0

The exact phrase 'knowledge security' was not found in the two journals, nor was the term 'knowledge' common in *Computers & Security*, in which only a handful of articles featured the word in any part of their text and it was completely absent from the articles' keywords. Most closely approaching knowledge security are articles about information security culture and management (von Solms & von Solms 2004a, von Solms & von Solms 2004b, Ruighaver et al. 2007). These papers employ a broad definition of information when they consider information security, knowledge included. The perspective, however, is similar to that in the information systems journals: an individual is mainly a subject of the various rules and policies the organisation has in place. There are also articles that specifically discuss the role of the user in information security (Stantona et al. 2005, Furnell et al. 2007, Furnell et al. 2008, Fuchs et al. 2011, Ifinedo 2012). In these pieces, the term 'knowledge' refers to the degree of knowledge a person has about the security policies. The word is also used in connection with computer systems communicating with each other (Lu & Liu 2009, Davis & Clark 2011), but in that case it is clear that the word 'knowledge' is not given the definition used in this work.

In *Information Management & Computer Security*, coming closest to the term 'knowledge security' is an article that takes a knowledge management perspective to information security. However promising its title, the approach involves not knowledge security but management of knowledge about information security (Belsis et al. 2005). The approach is very similar to that of Neef (2005), Massingham (2010), and Randeree (2006), described in the previous section. The authors stress that organisations do not give enough attention to knowledge of supporting functions, under which information security is classed. They concentrate more on managing knowledge about their core areas of business. Although the article does not discuss knowledge security directly, it raises some interesting questions, such as whether companies consider other knowledge than core business knowledge worth managing. Security is just one example of a supporting function that may not seem important from a business angle but that can prove essential for an organisation's success.

The systematic review did not yield enough search 'hits' to prove that there exists scientific discourse on the concept of knowledge security. Even the information security journals had no articles that could have used this term. However, the term has come up in several sources, so a way must be found to determine where it is used.

4.1.2 Database review

The third step in the conceptual analysis process (see Figure 7, on p. 14) is to find the various interpretations and uses of the concept studied. This third step is addressed by

this subsection, which reports on a literature review for the concept of knowledge security, performed to create a better understanding of where and how the concept is used. The search phrases used in this stage of the review were ‘knowledge security’, ‘knowledge’ near ‘security’, and ‘knowledge security management’. Later in the third stage, the review was complemented with exploration of parallel terms.

The main discussion arena for science is scientific journals. Therefore, a concept can be said to exist in science if it is used in journal articles. To get a good understanding of what has been published on the topic of knowledge security, the author performed searches of journal databases. Determining which databases should be searched is difficult, especially in this case, with a concept that clearly lies between two scientific fields: knowledge management and information security (or, in broader terms, information systems science). The former is itself a multidisciplinary field, embracing works in fields such as business administration, organisational learning, and social sciences. The latter also has multidisciplinary roots in computer science and many of the social sciences. Accordingly, the databases searched should cover these areas.

The databases selected for this review were the following:

- EBSCOhost
- Elsevier Science Direct
- Emerald
- Web of Science

Naturally, the search term used was ‘knowledge security’. The search results are presented in Table 14. The term ‘result item’ is used since not all of the results represent research articles. Some of the ‘hits’ are editorials, others short papers, some book reviews. Since the goal of the literature search was to find the uses and definitions for the term ‘knowledge security’, it makes sense to include instances of non-scientific or non-research use of the term also. The three articles reported on above that use the term ‘knowledge security’ are excluded from these results, since they have already been considered. The term ‘relevant items’ in Table 14 refers to the term ‘knowledge security’ being used in the text of the result item.

Table 14: Search results from the database review

Database	Result items	Relevant items
Elsevier Science Direct	50	6
EBSCOhost	5	1
Emerald	14	6
Web of Science	17	3
Total	86	16

Regardless of their presence in the result list, most of the result items either did not feature the term ‘knowledge security’ or used the two words within the document but individually rather than as a phrase – they happened to be close together and did not

together refer to knowledge security. Sometimes they were even adjacent, with a comma between them or one at the end of a paragraph and the other as the first word of the next.

The result items, 86 in total, were searched for the term 'knowledge security'. Sixteen items used the term in some role. Of the non-relevant items, most concentrated on data security, a field in which the word 'knowledge' is occasionally used to describe a shared state in communication between systems. The results also included some articles that had nothing to do with either knowledge management or information systems – e.g., articles on chemical substances or health care. These were the articles wherein the words 'knowledge' and 'security' just happened to be next to each other.

Below, all of the uses for the term 'knowledge security' that were found in the database search are presented. Some of the articles view knowledge as valuable *per se*, while others accept meta-knowledge – i.e., knowledge about other information and knowledge – as within the scope of protection. There are also differences as to whether the threat to knowledge originates inside the organisation or outside it. Some of the articles concentrate on security of knowledge in knowledge management systems, which in this study is considered application of a technical perspective on knowledge. The articles and their angles of approach to knowledge are listed in Table 15.

Table 15: Views on knowledge in articles that use the term 'knowledge security'

Article	**Knowledge as an asset**	**Meta-knowl-edge as an asset**	**Threats to knowledge from outside**	**Threats to knowledge from within**	**Knowledge as codifiable (technical perspective)**
Bose 2003	x		x	x	
Desouza & Vanapalli 2005	x	x	x	x	x (not exclusively)
Ross & Schulte 2005	x			x	x
Desouza 2006	x	x	x	x	x (not exclusively)
Ryan 2006a	x		x	x	
Ryan 2006b	x		x	x	
Ryan 2006c	x		x	x	
Czejdo 2007			x		x (data security)
Xi & Dang 2007	x			x	x
Baloh et al. 2008	x		x		x
Chen 2008	x		x	x	x
Fung & Fung 2008	x	x		x	

Article	Knowledge as an asset	Meta-knowledge as an asset	Threats to knowledge from outside	Threats to knowledge from within	Knowledge as codifiable (technical perspective)
O'Donoghue & Croasdell 2009	x		x		x
Ilvonen 2010	x	x	x	x	
Shedden et al. 2011		x		x	
Nassimbeni et al. 2012	x		x		x

Bose (2003) defines knowledge security as 'the measures taken to protect knowledge from accidental or intentional disclosure to unauthorized persons and from unauthorized alteration'. This means that Bose concentrates on knowledge that can be valuable to outsiders as it is, and that therefore needs to be secure.

Shedden et al. (2011) use the term 'knowledge security' differently: 'This paper will argue the need to move beyond the current asset focus within security through an exploration of knowledge security.' They argue that not just information assets need to be secure; additionally, knowledge about the assets and processes needs to be accounted for. This means that they consider the knowledge about processes to be valuable knowledge that must be protected from threats, arising mainly from within the organisation, as loss or unavailability of key employees. (Shedden et al. 2011)

Ross and Schulte (2005) use the term 'knowledge security' in connection with knowledge management systems. In their analysis, 'the study participants also indicated that multiple levels of knowledge, which independently can be used by many people collectively, might create a security violation, suggesting that [knowledge management] solutions must be able to manage multilevel knowledge security'. This implies that a threat to knowledge is created by overly open availability of knowledge to employees. However, their concern is about the openness of knowledge management systems, and the solution suggested is stricter access control and knowledge-entry classification. (Ross & Schulte 2005)

Fung and Fung (2008) too approach knowledge security from the knowledge management side. They stress that when knowledge sharing is among the main foci of knowledge management, security is a concern that needs to be addressed. Their paper discusses various elements of knowledge security and reviews implications in the context of the hospitality industry.

There is one article on the list that deviates from the definition of knowledge used in this study. Czejdo and Morzy (2008) use the term 'knowledge security' but actually are

referring to a modelling language to describe data security situations, in which the term 'knowledge' refers to metadata. Another article with a very technical orientation is a piece written by Chen (2008) in which 'knowledge security' is used as a term and a situation is described in which knowledge is especially embedded in people. The main focus of the article, however, is on knowledge management systems and the logic of how these systems communicate with each other.

Xi and Dang (2007) use the term 'knowledge security' in a paper that examines knowledge networks. They refer to knowledge as something that can be stored via either physical media or live media (i.e., in people): 'Generally knowledge stored in material media is safer than that in live media because employees may leave their jobs along with their individual knowledge, which threatens the knowledge security of organisations seriously. Therefore, knowledge stored in human brains gets more focus in the problems of knowledge security' (Xi & Dang 2007). This statement serves to point up the importance of the present study but also freed the authors of the article from having to discuss the concept of knowledge security further, since their focus was on studying the robustness of knowledge networks, not the phenomenon of knowledge security.

Also among those who mention the term 'knowledge security' are Nassimbeni et al. (2012), but they do not discuss the definition of the term. In their analysis of security risks that are related to services' outsourcing and offshoring, they state that 'companies have to manage several risks, and one of the most critical is data and knowledge security. These risks are so significant that many companies are reluctant to adopt outsourcing or offshoring for this reason' (Nassimbeni et al. 2012). The combination of data and knowledge security leads the reader to think about a technical orientation to knowledge, so, depending on how it is interpreted, the article could be categorised as non-relevant to the search. However, it was not rejected, since the intent of the authors is not entirely clear.

O'Donoghue and Croasdell (2009) mention knowledge security in the context of international operations. Their analysis 'considers existing literature and current practices to derive recommended practices on knowledge security in environments that may have weak protection practices in place'. The focus of the paper is on IPR protection. The term the authors use more in the paper is 'secure knowledge management', and they do not actually state what they mean when referring to knowledge security. They conclude that especially the knowledge that can be considered under the protection of intellectual property law may be considered safe in strong regulatory environments but that in weak regulatory environments the organisation needs to pay a large amount of attention to protecting that knowledge.

The main focus also of Baloh et al. (2008) is on outsourcing and partnering, and in this context they refer to knowledge security as one aspect of the agreements that need to be

made between companies that co-operate. The term ‘knowledge security’ is used only once in the paper and has a minor role there.

In an editorial, Desouza (2006) addresses knowledge security as an interesting research space. He defines knowledge security as lying between knowledge management and information security, although he situates knowledge management as a field within the larger field of information systems. This implies a technology-oriented view of knowledge management; however, Desouza points out, knowledge cannot be made secure by technical means only, as ‘most security breaches and competitive intelligence operations exploit non-technical weaknesses of an organization’ (Desouza 2006). Desouza calls for research on knowledge security and proposes a framework of people, product, and process for building of knowledge security (Desouza & Vanapalli 2005, Desouza 2006).

Ryan (2006a, 2006b, 2006c) has published three relevant short papers, of which two use the concept of knowledge security directly and one addresses the subject but does not use the concept itself. In the first short paper, Ryan emphasises the change that has led to security supply not corresponding with security demand. The supply provides technological solutions aimed at security of communications and computer systems, while the world is constantly moving towards more complex systems and more complex security needs. She argues that knowledge cannot be rendered and kept secure with the solutions now available; i.e., the security supply does not meet the security demand. If they are to be able to concentrate on innovation and knowledge sharing, companies need to address the security aspects of knowledge management. (Ryan 2006a)

In her next short paper, Ryan (2006b) argues that the key to knowledge security is the acknowledgement of tension between knowledge management and knowledge protection. While she writes about security of knowledge, however, she uses the keyword ‘data security’ in the keyword list and also in the text addresses issues such as losing a laptop computer or falling victim to a malware attack. (Ryan 2006b) This underscores the difficulty of deciding what falls under the definition of knowledge security. Important knowledge can be documented in computer systems, so technological means of protection are reasonable, but still the notion of data security or information security characterises the activity better. Although Ryan recognises that there are difficulties and challenges in security of knowledge, the paper does not address how these difficulties could be overcome. As one solution for finding balance between complete protection and no protection she suggests cost/benefit analysis considering the costs of protection against the expected benefits. However, she recognises that such cost/benefit analysis is akin to guessing, since there is little information available on the risks’ probabilities or the actual loss. (Ryan 2006b)

In the last short paper in the series, Ryan addresses the organisation’s politics as an aspect of knowledge security. She argues that the process of choosing security initiatives has more to it than just mapping of security needs to corresponding resources.

Many security needs cannot be quantified, so knowledge security becomes an issue more of architecture than of economics. Intangible elements such as organisational culture, social interests, and the organisation's politics constitute a large factor when one is dealing with intangible assets such as knowledge. Balancing diverse intangible needs that are difficult to quantify requires a qualitative approach. The knowledge security architect tasked with weaving knowledge security into an organisation needs to have the political skills to recognise and acknowledge the intangible needs of security in addition to the tangible ones. (Ryan 2006c)

Desouza and Vanapalli (2005) have built a framework addressing the perception that knowledge management literature does not address the security of knowledge, even though one of its stated aims is the exploitation of knowledge assets to their full potential. In the private sector, knowledge security is taken for granted. Desouza and Vanapalli (2005) draw examples from the defence and intelligence sector in building their knowledge security framework since no security, not even that of knowledge, is considered a given in that sector. Their framework is illustrated in Figure 30.

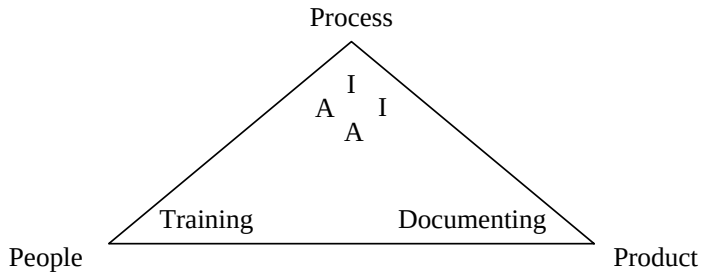

Figure 30: Knowledge security framework illustrated from description by Desouza and Vanapalli (2005)

The first part of applying the framework in Figure 30 is to address people, the source and carriers of important knowledge. Training and indoctrination, security clearances, and counterintelligence activities are suggested for the private sector too – of course, in reasonable proportion for the organisation. Knowledge as a product is addressed in the second part of the framework. Documentation is considered a key activity; when knowledge is documented, it can be brought under the umbrella of information security activities. Tagging and segmenting documents and keeping the devices with which knowledge is handled secure fall somewhat into the category of technical information security, but the knowledge standpoint is emphasised. (Desouza & Vanapalli 2005, Desouza 2006)

The process dimension of the framework presented in Figure 30 is the one most absent in the private sector, Desouza and Vanapalli (2005) argue. The process of knowledge security encompasses identification, authentication, authorisation, and integrity of knowledge (together 'IIAA' in Figure 30). Identification refers to the recognition and identification of an organisation's important knowledge assets. Authentication refers to the process ensuring that the company knows whom it is communicating with.

Authorisation refers to the process of contemplating carefully who has access to certain knowledge and how their use of that knowledge is logged. Finally, integrity is the dimension of maintaining the knowledge such that all changes to it can be tracked and only authorised changes are allowed (Desouza & Vanapalli 2005, Desouza 2006). The description in terms of process elements reveals that this framework is somewhat system-oriented, even though the authors are discussing knowledge. They concentrate mainly on knowledge that is stored in knowledge management systems. Authentication and integrity are approached from a perspective that is typical for an information systems environment, although the authors do draw analogies also to activities that take place outside the systems. The framework presented in Figure 30 bears much relation to the knowledge management factors of people, process, and technology presented by, for example, Awad and Ghaziri (2004) as depicted in Figure 13 (on p. 30).

The more usual and older use of the concept of knowledge security is in the context of information systems and the information transfer in them. For example, Boella and van der Torre (2006) refer to knowledge security in relation to the policies stating how the technological tools of virtual communities are allowed to communicate with each other. However, in their definition for the concept of knowledge they diverge quite a bit from the lines of this study.

Ryan (2006b) and Desouza (2006) have brought the concept of knowledge security into the consciousness of their respective research communities via editorials and viewpoint articles, and Desouza and Vanapalli (2005) have taken empirical steps to prove the relevance of knowledge security not just in the defence and intelligence sector but also in business. The phenomenon of knowledge security exists and is certainly not entirely new.

Among the result items from the above-mentioned database searches were a few items that presented a review of Desouza's book *Managing Knowledge Security*. Desouza (2007) supplements the term 'knowledge security' with the subheading 'Protecting a company's intellectual assets'. He applies a definition for the concept of knowledge that is somewhat similar to the one used in this study, and knowledge security is defined as an activity that protects important knowledge of the organisation against both external and internal threats. The practices of protection that Desouza introduces range from keeping the working space clean to providing awareness training of employees and managing intellectual property rights well. For him, employee awareness of what is important knowledge and of how each worker can contribute to its protection is essential (Desouza 2007).

In summary, some discussion in the literature does use the term 'knowledge security'. Perspectives vary from management of knowledge about risks and security to actual management of the security of knowledge overall. The articles emphasise the role of people as both holders and users of the knowledge and as threats to knowledge. The point of view in the discussion seems to be that of the issuer of a 'wake-up call'.

Companies, according to the articles, are not addressing the various aspects of knowledge security as well as they could.

Awareness of risks, both among the management and on the part of each employee, could be higher, and the emphasis with the term 'knowledge security' is aimed at inspiring people to think about threats and possible solutions to them. However, the articles provide little advice as to what companies need to do about knowledge security. Most instances of use of the concept occur in connection with the idea that this is something that needs to be addressed, but the authors of the articles do not concentrate on that. The present study, in contrast, is conducted as an attempt to define the concept of knowledge security 'head-on' and determine what should be done in companies to address their knowledge security needs. Before that, however, the concepts parallel to knowledge security need to be examined.

4.2 Parallel concepts

The systematic literature review presented above included analysis of parallel concepts to knowledge security, such as knowledge risk and knowledge protection. In addition to exploring these concepts, this section is aimed at broadening the perspective of the conceptual analysis beyond the main informing theories that were presented in Chapter 2. At the same time, this section communicates the study's limitations by briefly introducing areas of research that, while not considered to lie within the boundaries of the focus of this study, can be claimed to have a relationship to the concept under analysis. The discussion of these parallel concepts contributes to the theoretical framework for the concept of knowledge security by making the limitations and relationships clearer.

4.2.1 Competitive intelligence and counterintelligence

Competitive intelligence and its complement, or counterpart, counterintelligence can be seen as the first parallel concepts to knowledge security. Competitive intelligence (CI) is a process aimed at gathering, enriching, and sharing of information and knowledge about organisations' competitive environment (Collins 1997, Thierauf 2001). As a process, CI is the set of legal and ethical methods a company uses to harness information that helps it gain and maintain a competitive position. This process consists of phases such as identifying information needs, gathering information from various sources, analysing the information, distributing it, and using it in decision-making (Collins 1997, Choo 2002, Vitt et al. 2002). The name 'CI' is used also to denote the product that is the outcome of the CI process; that is, CI is also information and understanding about competitors' activities, gleaned from public and private sources, and its scope is the current and future behaviour of competitors, suppliers, and

customers, along with effects of technologies and other market activities (Vedder et al. 1999).

When companies aim to enrich and spot important pieces of knowledge, they need to recognise them (Drott 2001); determination of the information needs is an important part of the CI process (Wilson 1994, Devadason & Lingam 1997, Nicholas 2000). Judging a piece of information to be needed requires that it be recognised as important. The link between knowledge security and competitive intelligence is found in knowledge recognition: valuable bits of knowledge need to be found. From the point of view of CI, their recognition is important, allowing the knowledge to be found and utilised in creation of an accurate picture of the competitive situation of the company. From the security angle, this recognition is important for ensuring that the important knowledge can be kept secure against threats of leaks or loss of the knowledge.

Counterintelligence refers to reactive and proactive measures to prevent critical information from reaching the eyes and ears of a competitor. The counterintelligence function can be regarded as complementary to the security function of an organisation (Desouza & Vanapalli 2005) or may be performed by the security department. Counterintelligence is sometimes replaced with the term 'defensive intelligence' in the literature, mainly for ease of abbreviation of the terms in an article that discusses both competitive intelligence and counterintelligence. In their article, Helms et al. (2000) define defensive intelligence as an activity that engages and neutralises a competitor's information collection efforts through a system of countermeasures. Counterintelligence is defence against the competitive intelligence activities of competitors (Helms et al. 2000). Therefore, it is in a way a subset of the information security activities. The information security goal of a company is to protect information against all risks, regardless of where they originate (Whitman & Mattord 2003, Peltier et al. 2005, VAHTI 2009).

When companies take counterintelligence measures, they take risks at the same time. A concern of many companies is the spending on activities that do not provide a direct benefit for the organisation. According to Helms et al. (2000), some of the measures are tangible and easy to comprehend and measure, among them physical guarding and surveillance systems. The more difficult and potentially expensive counterintelligence solutions deal with limiting the free flow of information within a company. Although limiting access to information may not be an expensive solution *per se*, it can lead to costs for the company in the long run through inefficiency, duplication of effort, and lack of communication. (Helms et al. 2000)

The key element connecting knowledge security and counterintelligence is the role of people and their behaviour in conducting the activity. Counterintelligence efforts should include promoting employees' awareness about valuable information and its protection (Helms et al. 2000). Counterintelligence is rooted strongly in the recognition of important knowledge. The competitive intelligence process in companies concentrates

on the kind of knowledge that the organisation wants to have about its competitors (Fuld 1991, Collins 1997, Herring 1999, Frishammar 2003). This recognition offers guidance for knowing what knowledge needs to be kept secure from competitors within the company itself – i.e., for counterintelligence. Both of these processes, competitive intelligence and counterintelligence, deal with information and knowledge, and this places them in close relation to knowledge security.

4.2.2 Knowledge protection

Knowledge protection and knowledge security are, when used as terms, very close to each other. In the case of this parallel concept, the point of examination is to find the differences between the concepts, just as much as the similarities. The differences between the two concepts show one way to clarify the limits and focus of this study.

Many authors consider knowledge protection an integral part of knowledge management (Davenport et al. 1998, Gold et al. 2001, Lucas 2010, Maier 2010). The field of knowledge management, therefore, adopts a security-based perspective on knowledge. However, many articles that address protection as an important part of knowledge management leave it outside the scope of their research or do not discuss the protection mechanisms much beyond the level of a few questionnaire elements (e.g., Gold et al. 2001, Donate & Canales 2012). In consequence, the perspective of protection that the knowledge management field provides is a good starting point for further analysis of which elements fall under the concept of knowledge security.

Gold et al. (2001) discuss protection of knowledge as one knowledge process that companies carry out. They list 10 items that they consider to reflect knowledge protection as a process at a company (Gold et al. 2001, p. 200). These items are used further by other scholars in studies of knowledge management capabilities (e.g., Sandhawalia & Dalcher 2011, Ding et al. 2013). The items listed by Gold et al. (2001) are

- processes to protect knowledge from inappropriate use within the organisation
- processes to protect knowledge from inappropriate use outside the organisation
- processes to protect knowledge from theft originating within the organisation
- processes to protect knowledge against theft from outside the organisation
- incentives that encourage the protection of knowledge
- technology that restricts access to some sources of knowledge
- extensive policies and procedures for protecting trade secrets
- the organisation valuing and protecting knowledge embedded in individuals
- clear identification of the knowledge that is restricted
- clear communication of the importance of protecting knowledge

These items show a division between two sources of threats: internal and external to the company. The items also communicate that the main threat to knowledge is theft or inappropriate use, which can be interpreted to be essentially the same thing. The list

also communicates the idea that the knowledge important to companies is related to trade secrets. One item, however, does also consider knowledge that is embedded in people, while the other items can be interpreted as to do with protection of codified knowledge in the main.

The authors de Faria and Sofka (2010) divide knowledge protection into two areas: formal and strategic knowledge protection. Another way of classifying knowledge protection mechanisms is presented by Norman (2001). In this classification, the protection mechanisms are related to human resources, legal structures, and processes. Also, in Norman's classification the formal, or legal, protection mechanisms are mentioned as one key way to protect critical knowledge of companies.

Formal means of knowledge protection are legally oriented means: patents, copyrights, and trademarks are ways of protecting knowledge formally from use by competitors (Liebeskind 1997). A patent provides a temporary monopoly through which a company can benefit from an invention (Mansfield 1986). Copyright protects a company's product content from replication. The problem with these legal means of protection is that they require extensive documentation of the important knowledge in the first place (de Faria & Sofka 2010). Other legal means to protect knowledge are contracts. Companies that decide to form partnerships with other companies need to pay close attention to what kinds of legally binding agreements they make pertaining to the knowledge that is shared with the partner. The contracts must specify what information and capabilities may and may not be shared, and they also specify consequences for violation of the contract (Norman 2001).

The context in which legal knowledge protection mechanisms are discussed in the literature is mainly that of multinational companies and strategic alliances between companies (Norman 2001, Baloh et al. 2008, O'Donoghue & Croasdell 2009, de Faria & Sofka 2010). The knowledge that is considered critical is connected to research and development activities. This implies that the knowledge is created within the product development process and thus able to be patented or otherwise protected with contracts. Knowledge codified in patent applications is beyond the scope of this study (see Figure 11, on p. 28); accordingly, the formal knowledge protection mechanisms too are considered to lie mainly outside the scope of this study, although it is acknowledged that they are something a company needs to consider in order to protect its knowledge.

The other knowledge protection mechanisms, which de Faria and Sofka (2010) refer to as strategic protection, are aimed at the absolute protection of knowledge. While the legal protection mechanisms more or less require explicit codifying and sharing of the knowledge (Mansfield 1986), the strategic protection mechanisms are based on secrecy and complexity of knowledge and product designs (Norman 2001, de Faria & Sofka 2010). As has been mentioned above, knowledge is more easily kept secret when it is not documented in any patent applications or contracts, and when the product designs and knowledge required for understanding the products are complex enough, those

products are harder for competitors to imitate and copy. Protecting knowledge by keeping it secret requires training of employees such that they are aware of the value of the knowledge for the company (Norman 2001); however, these protection mechanisms too have been studied mainly in the context of strategic alliances and R&D collaboration (Hurmelinna-Laukkanen 2011).

Knowledge protection as a concept is quite close to knowledge security. The use of the term seems to be connected to alliances between companies, and knowledge protection is performed in order to prevent knowledge spill-over. What is considered knowledge under the term 'knowledge protection' can be examined too: the definition of knowledge used in this study emphasises the ties between knowledge and people. Attempting to protect knowledge by formal legal measures implies that knowledge is an asset that can be codified and separated from people. This makes the target of protection closer to information than knowledge by the definitions used in this study. However, the strategic knowledge protection mechanisms address also the knowledge bound up in people and acknowledge the complexity of knowledge. This is why these knowledge protection mechanisms can be considered a close parallel to knowledge security.

The threat perspectives and protection mechanisms presented by knowledge protection literature take a narrow view of knowledge in the sense that the main threat is considered to be knowledge leaks to competitors. Although that is considered a major threat in this study, the information security literature acknowledges that there are many other threat situations than just the leaking of information. In the introductory empirical material too, it was acknowledged that leaking information outside the company may be a well acknowledged threat but is not necessarily the biggest threat and certainly is not the only one. When this perspective is considered in parallel to knowledge, the concept of knowledge protection seems to be quite narrow. The knowledge protection perspective that is studied in the context of strategic alliances is something that certainly can be utilised also in other contexts. However, the angle of threats that knowledge is protected against is quite narrow if leaks are considered the main threat to knowledge.

4.3 Knowledge security – a theoretical definition

The literature review work presented in Section 4.1 shows that even though knowledge security is not a widely used concept, its use can be reasoned. The articles that do use the concept call for activities that make better use of the knowledge and that better protect the knowledge that companies possess. There is a need to discuss not only the security of companies' information but also the security of the knowledge, which is considered in many articles to be one of the most important assets a company can have.

Security can be regarded as a process aimed at reaching a secure state. The basic dynamics of this process are illustrated in Figure 3, on page 8. In that figure, knowledge security emerges from the managerial actions intended to protect important knowledge

within an organisation. In addition to considering knowledge security as a process, one can argue that the characteristics of confidentiality, integrity, and availability apply in knowledge security. These characteristics are analogous to those from the information security field, and they provide a tested and reasoned framework for examining the characteristics of knowledge from the security perspective. The desired characteristics are presented in Figure 31.

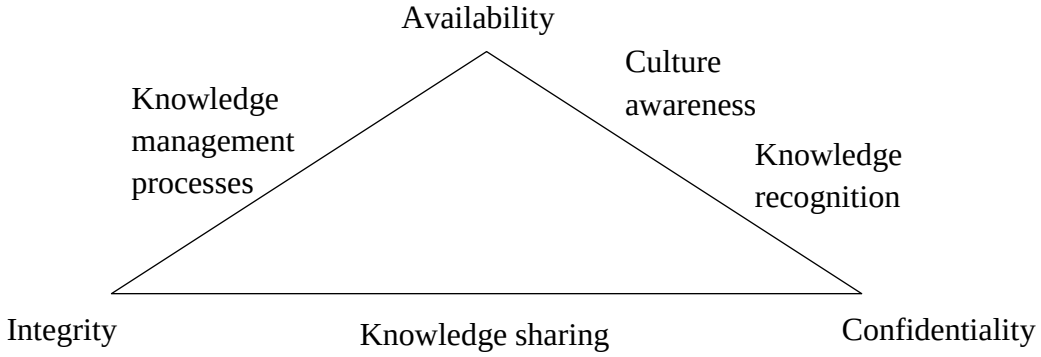

Figure 31: The CIA approach to knowledge based on theory

Knowledge management processes are aimed at such objectives as the codification of knowledge, and through the pursuit of this aim they assist in maintaining the availability and integrity of knowledge, as presented in Figure 31. Although not all knowledge can be codified, at least some codification should help in keeping knowledge available to other employees when the person who initially possessed that knowledge is not present. The processes can also be a good way to ensure integrity of knowledge, through spreading of knowledge about work processes, product configurations, etc. to more than one person via the aid of information systems. The crowd who utilise the knowledge can also work as a community ensuring that the knowledge documented in the system is up to date. From the perspective of this study, the codified knowledge is not the main result of codification. The main result is work processes that encourage people not only to write down their experiences but to communicate with co-workers about the codified knowledge.

Sharing knowledge within networks inside the organisation can serve as one way to ensure availability of knowledge, as is illustrated in Figure 31. However, networking can also operate as a way to ensure the confidentiality and integrity of knowledge. The reservoir model of Argote and Ingram presented in Subsection 2.2.2 suggests that one solution for avoidance of knowledge spill-over to competitor organisations is to embed important knowledge in subsidiary networks that involve people. Knowledge embedded in these networks is less likely to be transferred to other organisations, for studies have shown knowledge transfer to be more difficult when the knowledge is embedded in networks involving people and a certain division of labour (member–task networks) or that involve certain people using a certain set of tools (member–tool networks) (Argote & Ingram 2000). This mechanism is described in different terms by de Faria and Sofka

(2010), who argue that knowledge can be protected by limiting the amount of knowledge each actor in an alliance has and making the combination of individual knowledge products complex and hard to copy. Sharing knowledge in limited ways and adding complexity and layers (member–task and member-tool) is a means of strategic knowledge protection.

Culture and awareness have a strong role in the concept of knowledge security. In the 'map' of critical characteristics of knowledge in Figure 31, the culture is connected mainly to confidentiality of knowledge. When employees are aware of which knowledge is important, they are more likely to protect that knowledge. The recognition of important knowledge favours security of all the characteristics, but the link is perhaps the strongest to confidentiality. In addition to confidentiality, recognition of important knowledge is a prerequisite for making that knowledge available to those in need of it.

The basic elements of the CIA triangle for knowledge in Figure 31 may not appear any different from those in the context of information security. Indeed, the basic idea of this approach is the same, and there is little difference between the characteristics approach to information and to knowledge. In the case of knowledge, the dependence of the characteristics on human action is more evident than in the information security context. In the case of data and information, many of the mechanisms for protection of the characteristics can rely on technical solutions such as backup copies and access control. In the case of knowledge, the technical solutions are only one small element in the protection, since backing up an individual's knowledge and experiences is impossible.

In addition to the perspective of characteristics presented in Figure 31, the perspective of threats can be applied to knowledge, and this perspective can be seen in the literature. Knowledge is protected against threats by the means of security management and knowledge protection. The threats from outside the organisation target knowledge, because it can be extremely valuable to, say, a competitor. It may also be easier to obtain than sensitive data lying behind high barriers of protection by technical means. Threats from inside can stem from, for instance, disgruntled employees leaking important knowledge to competitors. Threats caused by employee absence or personnel turnover can also be considered internal threats to knowledge. The threat-oriented perspectives on knowledge are illustrated in Figure 32.

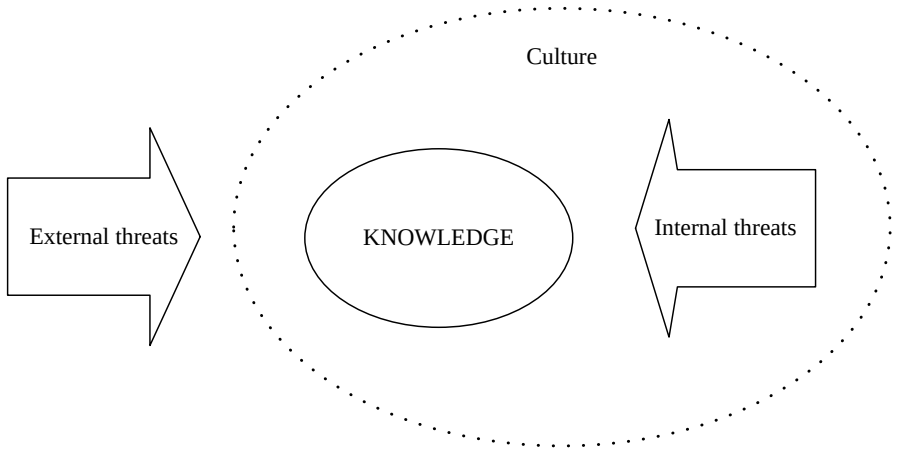

Figure 32: Threat-based perspectives on knowledge

The main external threat to knowledge presented in Figure 32 is the competitors. Competition is what makes the knowledge of an organisation interesting not only to its competitors but to crackers and other outsiders. Depending on the industry of the organisation's operations, other motives for obtaining knowledge from within the organisation may, of course, exist, such as national and political motives.

The internal threats to knowledge presented in Figure 32 can be further divided into threats of loss and threats of leaks. The latter category is an extension of the external threat of competitors or other parties being interested in knowledge that is important to the organisation. These threats can be actualised through the actions of an insider working for the organisation, whether by conscious or by unintentional action. The culture and awareness are major drivers of improved knowledge security in this regard. When people are more aware of the threats they can accidentally cause to the knowledge of the company, they pay attention to their actions. Also, the awareness of possibilities of intentional harm may reduce the threat of it occurring, as informed and aware employees keep an eye out for unusual behaviour within the company. The threat of knowledge loss within the organisation can become reality through employee turnover, and in many cases it is tackled at least partly through knowledge management initiatives.

Knowledge security in this study is defined as *the process of securing the knowledge of people working at a company*. These people possess important knowledge both as individuals and collectively, and the knowledge resides also in processes of conducting the work and in technological tools that the workers use. Knowledge security is aimed at keeping this knowledge secure from other parties who could benefit from it (competitors, criminals, etc.) and also at guaranteeing the availability and integrity of that knowledge within the organisation. The parallel concepts presented in sections 4.1 and 4.2 have their own common uses that are complementary to knowledge security though not identical to it.

We can state, as a conclusion on the theoretical definition and theoretical model for the concept of knowledge security, that knowledge security is the process of protecting knowledge of an organisation against internal and external threats. This process is aimed at maintaining the ideal characteristics of knowledge in all situations, and it considers all contexts wherein important knowledge is handled. This extends the knowledge protection mechanisms described under the parallel concepts from the context of business intelligence or from the context of strategic alliances to all companies and all kinds of operations.

5 The primary empirical study

The second research question presented at the beginning of this study is answered primarily through the empirical work described in this chapter: How do companies secure knowledge?

This research question can be further divided into sub-questions such as these: What is important knowledge for companies? How do they recognise this knowledge? What do they do to protect this knowledge?

In this chapter, the findings from the empirical material are presented and the analysis trail is illustrated. The key findings are summarised in the final part of the chapter. Steps 3–6 of conceptual analysis as presented in Figure 7 (see p. 14) are followed for the second iteration in this section. The parallel concepts identified in the previous chapter of the work are searched for in the interview material (step 4). Then, the characteristics of the concept of knowledge security are analysed in light of the interviews (step 5), alongside tentative uses for the concept (step 3). Finally, an empirical model for the concept is built (step 6).

5.1 The research setting

In this section, the research setting is introduced. The empirical material consists of interview data, so the interview arrangements and themes are introduced as background. Also, the analysis method is presented in brief.

5.1.1 Interview arrangements

Interviews were carried out at both large and mid-sized organisations. The security manager or knowledge manager of the companies (in smaller companies, the CEO) was contacted and the interview proposed. The companies were selected by size and industry such that the sample encompassed companies of various sizes and that were active in different industries, to provide rich viewpoints on knowledge security. Out of 15 companies contacted, seven agreed to participate in the interviews. The companies were guaranteed anonymity; accordingly, no company-specific results will be published. Since Finland is a small country, neither are the specific industries and locations of the companies reported, as this information would practically identify the individual companies. The companies ranged in size from 100 to 3,500 employees. Their industries include high technology, consulting, heavy manufacturing, and consumer product design and manufacture.

The companies were asked for interviews with the people responsible for knowledge management and information security management. On account of schedule difficulties,

this setting was not possible in every company, so in some cases there was only one interviewee. The number of interviewees at each company and the position of each are listed in Table 16.

Table 16: List of interviewees

Company	Interviewees
P1	H1: Security manager H2: HR and KM manager
P2	H1: CEO H2: Vice-CEO H3: Board director H4: Marketing manager
P3	H1: HR manager H2: CIO H3: Information manager H4: Information security manager
P4	H1: Information, security, and KM manager
P5	H1: Information security manager
P6	H1: HR director H2: Production manager
P7	H1: Information security manager

At two companies, there were four interviewees; there were two interviewees at each of two companies; and in three companies, there was only one interviewee. The interviews were conducted in the Finnish language and also transcribed in Finnish. In the following analysis, extracts from the interviews are used as examples, to illustrate the line of analysis. The author of this study translated the excerpts for presentation here.

5.1.2 Interview questions

The interviews were arranged as themed interviews. This means that no pre-structured questions were presented; instead, the interviewer encouraged the interviewees to describe practices at the companies. The aim with the interviews was to gain understanding of the existing phenomenon that in this study is called knowledge security but to which a company may give other names. This is why pre-structured questions were not used and the informants were not given definitions detailing what knowledge security means for the author. The term ‘knowledge security’ (‘tietämyksen turvaaminen’ in Finnish), however, was used in the interview material, and if asked, the interviewer would explain the general idea of the doctoral research to the interviewees in explanation of the term. That general idea is expressed as being to combine the approaches of knowledge management and information security management and, in so doing, arrive at a definition for the concept of knowledge security.

Although the interviewer would not share her view of the term subject to conceptual analysis, the interviews were begun with discussion of what the word ‘knowledge’

means. This was done to ensure that the interviewees understood what the interviewer meant by the term and what she was interested in. This clarification of interest was important, because the interviewees seemed to have the same, quite technically oriented view of information security as the interviewees in the introductory study. In clarifying that the element of interest was knowledge, the interviews challenged the interviewees to think beyond the technical boundaries usually delineated for information security.

At this point, it is relevant to reiterate that the interviews were conducted and analysed in Finnish. The terms used were 'tietoturvallisuus' and 'tietämys', meaning 'information security' and 'knowledge', respectively. As is stated in the introduction to this study, *tieto* is a general concept that has the potential to cover also knowledge. The interviewees would most often use the term 'tieto' in their examples. The translation given here, into either 'information' or 'knowledge', depends on the context of the answer, and in this translation the author interprets what the interviewees meant in their use of the term.

The interview themes were chosen on the basis of the fields of theory that informed the work. The concept of knowledge security is situated between the fields of knowledge management and information security management. The information security management frameworks emphasise these themes in the manner in which the elements of identifying the asset to be secured and of then identifying the threat to that asset were present. The knowledge management perspectives on knowledge, as presented above, were also utilised in formulation of the interview themes. The original list of themes, in Finnish, is found in Appendix 2.

Interview themes

Knowledge, and information and knowledge security

- The concepts used in connection with information security
- The concept of knowledge
- Information security actions
- Threats against which information and knowledge are protected

Knowledge and its recognition

- Valuable knowledge
- How valuable knowledge gets recognised
- Criteria for recognition
- Classification of knowledge
- Tools for knowledge classification
- Use of the cube model for knowledge recognition and classification

Knowledge management and knowledge security

- Knowledge management practices
- Roles of KM and KS, co-operation / competition

Knowledge security practices

- Knowledge security instructions vs. information security instructions
- Secure behaviour and instructions for it
- Knowledge sharing practices and instructions
- The knowledge sharing mindset: to share or to keep
- Knowledge sharing tools and instructions
- Changes in knowledge sharing practices
- Knowledge security initiatives, if any

The themes were covered in all interviews, although the depth of discussion of each theme differed between interviews. The interviewer's aim was to inspire discussion especially in the group interviews. Each interview lasted approximately one hour. This time was enough for going over all the themes but not enough for in-depth discussion of them all. A longer discussion might have been more fruitful from the standpoint of this study, but the amount of time that the interview required seemed to be a major factor in the companies' decision on whether to participate or not. Although the interview required only an hour, some companies declined the request with an explanation that they did not have the time. Another reason given for declining to take part in an interview was that company policy would not allow discussion of information security practices with someone from outside the company, not even with the guarantee of anonymity.

The interviews were conducted, recorded, and transcribed by the author. The recording helped to capture the exact expressions the interviewees used, along with the interplay between the interviewees when there were more than one of them. The interviewer did take notes during the interviews, but these were more for the purpose of following the interview themes through than for documenting observations about the interviews.

5.1.3 The analysis method

This section introduces the methods used in the analysis of the empirical material. Both inductive and deductive approaches to the material were used. The content analysis method used in this study was introduced more fully in Subsection 3.1.3 of this study.

The transcribed interviews were analysed with the aid of the qualitative analysis software ATLAS.ti. All transcribed material was read with the software, and extracts from each interview were tagged under the various interview themes. This more or less follows the structured and deductive content analysis process (Jauch et al. 1980, Guthrie

et al. 2004, Hsieh & Shannon 2005, Elo & Kyngäs 2008). The interview theme list worked as an initial analysis structure, and many of the themes were used as coding categories.

The excerpts were then grouped into sub-categories under each theme. After the interviews were broken down into small sections, placed in various categories, these categories were analysed for determination of what kind of bigger picture could be built from them. For example, an excerpt first coded under the theme 'threat to knowledge' could be more specifically placed under the code 'employee turnover'. All extracts under the 'threat to knowledge' label would then be analysed, and common sub-categories discussed in the write-up. This method describes in a way the conventional content analysis process of codes emerging from the material (Hsieh & Shannon 2005, Elo & Kyngäs 2008). In this, the primary empirical study takes both a deductive and an inductive approach to content analysis, as was the case with the introductory empirical study.

5.2 Findings from the interviews

The following discussion presents and explores the main themes that emerged from the theory and the interview material. Quotes from the material are presented to illustrate how the interviewees discussed the themes and to show how the researcher has analysed them. The interview themes were constructed around the parallel concepts that have been identified in Chapter 4, because the literature review showed the concept of knowledge security to be used little, even in the scientific literature. Therefore, it is safe to assume that the term is not used in everyday business, and indeed the term was not familiar to the interviewees.

In the sections of the work that follow, the blocks of italicised text consist of translated quotes from the interview material. The translations were performed by the author and are not necessarily word for word. Instead, translation was done in the manner best expressing what the interviewees said. Many figures of speech do not translate directly from one language to another. An example can be seen in the following quote:

> ***P1*** *H1: But we instruct in behaviour and tell people not to be naïve.*

In this case, the word 'naïve' is used instead of the direct translation 'blue-eyed'. To an English-speaking reader, the former better conveys what the interviewee means; the expression 'blue-eyed person' is used often in the Finnish language to refer to a person who is naïve or not critical in his or her choice of behaviour.

All of the excerpts begin with a letter-number combination that is highlighted through application of boldface. This combination, **P2** in the following example, signifies the company the extract comes from.

> ***P2*** *H2: [Important knowledge is] that we have different areas where we apply solutions. I mean how information is used for solutions in the circumstances we are in.*
> *H3: […] Especially knowledge about how to get from information to knowledge. It's meta-knowledge.*

The above quotes serve as one example of an extract drawn from an interview that may include many statements, from several interviewees – and that many times, it is the discussion between the interviewees that makes the excerpt interesting. In some cases, the interviewer (in the case illustrated above, the author of this study) participated in the discussion. Again, the interviewer is represented with the letter 'I' in the quoted material. The interviewees and the position of each at his or her company are listed in Table 16.

5.2.1 Important knowledge

The first theme that we can trace as we begin the analysis of knowledge security from the interview data is recognition of important and valuable knowledge. Recognising important knowledge is the first step toward security of that knowledge, so it is very important that people who make decisions about security activities have a very good picture of what knowledge is important for the company. With this theme, different views as to which knowledge is important for the company were found at the companies that had multiple interviewees. Any given company may have mentioned all three sub-categories of important knowledge presented in Table 17 or just one of them.

Table 17: What was deemed to constitute important knowledge

Sub-category of the important knowledge	The definition	Instances
Product and development knowledge	The knowledge that is used for developing and producing the company's products is the most important knowledge	7
Knowledge about the customers	Understanding what the customers need and being able to translate that need into products and services is of the greatest importance for the company	5
Knowledge about processes	In addition to knowledge that is used for developing the products, there is a large amount of important knowledge about how to organise activities such that the products can be developed and produced	5

The interviewees identified several types of important knowledge, but knowledge about products and development was mentioned as the most important. The products and development sub-category under the theme of important knowledge includes extracts from all seven companies studied, as can be seen from Table 17.

> ***P4*** *H1: We feel we are the world leader today. We have this product offering that forms the core around which our business is constructed. And all the knowledge that is connected to it and how it works and how it needs to be handled. So if I need to mention something above all others [as important knowledge], then that's it.*
>
> ***P5*** *H1: Valuable knowledge in this context is summarised as the way we see the world and how we build the services we provide.*

These quotes represent the 'product and development knowledge' category of important knowledge. The interviewees prioritised the knowledge of their product offering and the research and development that is behind it as the most important knowledge for the company. The interviewee for company P4 felt that knowledge pertaining to the company's world-leading product offering is what is most important for the company. The interviewee from company P5 expressed the same approach briefly by saying that valuable knowledge is, on one hand, a mindset of seeing the world in a certain way and, on the other, ability to put that mindset to use to create products and services. The rest of the answers in this category display variations of these two approaches.

Although the companies differ greatly by industry, knowledge about product development is still considered most important. This is not surprising; common sense says that knowing how to develop a product that meets customer expectations is essential. In this regard, it does not matter whether the product is a service, a physical appliance, or a combination of the two. The connection to customers was further emphasised at some of the companies:

> ***P6*** *H2: Service is an important part of our business. We are talking not about traditional after-sales marketing but about various service packages.*
> *H1: Process support.*
> *H2: And you just can't sell that if you don't understand what the customer really needs.*

In a business-to-business setting, understanding the needs of the customers is essential, and also the connection to one's customers can be very close. As this extract representing the 'knowledge about customers' category illustrates, understanding customers is considered vital. With consumer products, the connection to the end customer is not as close and knowledge about the customer relationship may not be considered so critical. The company may be developing certain products without listening to what the customers want, and thus creating demand for the product by offering the customers something that they did not know they wanted.

All of the companies that participated in the interviews engage in in-house product development, which provides them with a competitive position in the international

market. On the global scale, the companies are quite small, with 100 to 3,500 employees each. Their smallness does give them an advantage: they can offer flexibility that is not possible for larger corporations. They also have employees who possess a broad-based understanding of the entity of their business processes. Also, knowledge and understanding of how things are done is important for the companies.

> ***P1*** *H1: Then we have in the bigger unit knowledge about the industry and customer relationship, and knowledge about activities and systems. There are people who have really special knowledge.*
>
> ***P2*** *H2: [Important knowledge is] that we have different areas where we apply solutions. I mean how information is used for solutions in the circumstances we are in.*
> *H3: And I think this is one part of our knowledge, especially knowledge about how to get from information to knowledge. It's meta-knowledge.*
>
> ***P3*** *H4: I would take also another point of view: we have now been talking about products, but if we were now to build a new factory, the building process does not have much to do with our product, but still we have a lot of knowledge about how to set up the infrastructure. And that is valuable knowledge in its own right.*

In these extracts representing the 'knowledge about processes' category, the interviewees stated not only that their competitive position was based on a good product and new-product development. They also emphasised that understanding how to carry out this development and how to build processes is important. This knowledge forms the foundation on which efficiency and productivity are built. This process-related knowledge can be linked to, for example, the infrastructure and organisation of the company, the relationships of the company to the industry as a whole system, or problem-solving in general. Knowledge about how the company works, how it has been built, and how problems are solved is valuable to these companies in addition to the knowledge that is directly linked to production of the product offering.

5.2.2 Knowledge recognition

Recognising what knowledge is important for the company is not always straight-forward. With the discussion presented above, the interviewees were asked themselves to identify what is important and valuable knowledge for the company. The next step is to find out how the company knows what knowledge is important – i.e., who in the company actually recognises valuable knowledge. The categorisation of knowledge recognition is presented in Table 18.

Table 18: Categorisation of knowledge recognition

Sub-category to knowledge recognition	Definition	Instances
Human relations perspective	Important and valuable knowledge is identified by the managers of the company, and the human resources of the company are assigned and trained on the basis of this recognition	3
Single-worker perspective	Individual employees are responsible for recognising knowledge that is valuable to the company and the associated confidentiality requirements	4

The interviewees took different approaches to recognition, depending on who was answering the question. The human relations angle on recognising important knowledge placed its emphasis on competencies: what competencies are important for completing the work and reaching business objectives. This perspective emphasises the networked or collective nature of an organisation as a collection of individuals with skills, knowledge, and competencies.

> ***P3*** *H2: We should find the internal knowledge that has so much importance that if we lost it, we would end up in a catastrophe. We will not find that knowledge outside the organisation [if we lose it].*

> ***P2*** *H4: [I]t's not someone [who recognises important knowledge]; it is a multidimensional process of discussion by many combinations of people.*
> *H2: It also depends on the area and level where the knowledge resides.*
> *H1: This company is an organism, and when an organism contains many cells, the network of cells can operate well, but an individual cell is quite helpless […].*
> *H4: We have a group of people here who have the core knowledge. Then we have a group of 'outsiders' who have a definite sector of knowledge covered. And I think that strategically important knowledge is created by bringing the outside knowledge and understanding into the inside group, who evaluate the knowledge and reflect on it in relation to the strategy. And I feel the inside people look quite strictly at what knowledge is top secret, intimate knowledge and whom they trust with that knowledge.*

It is evident in the human relations view of knowledge recognition, as presented above, that knowledge recognition is not a finely defined everyday process at the companies. The human relations perspective on important knowledge recognition implies that there are certain people at the company who know through discussions which of the knowledge is valuable. The task of the managers is to identify the people who have important knowledge and also to recognise where the knowledge is discussed.

Another way to approach the recognition of important knowledge is to think about it from the perspective of individual employees and how they recognise their knowledge

needs. The employees themselves are many times responsible for recognising valuable knowledge in terms of confidentiality. The interviewees indicated that the knowledge valuable to the company is confidential in nature. The individual employees are responsible for recognising that confidential knowledge and treating it accordingly.

> ***P1*** *H2: [T]he strategy comes from above, and it is carried all the way to the individual product lines, and the product line managers will have development discussions with employees, and in those discussions they will go over what is expected from the expert. The employees themselves are the experts; they know what knowledge they need to perform the task. An expert organisation is not a pyramid; it is a flock, or a school of fish. The observations of an individual influence the whole group, and the group is smarter than the individuals.*

This quote representing the 'single-worker perspective' category of knowledge recognition differs from the rest in its category in that it does not emphasise confidentiality as a criterion for valuable knowledge. It nonetheless belongs to the category of individuals recognising important knowledge, because the emphasis is on the process of people being the experts on what kind of knowledge they need and will need for their work. The interviewee in question compared the company of experts to a school of fish – any individual can, through his or her observations, change the behaviour of the entire company on the basis of these observations.

> ***P4*** *H1: [M]any people have their own tasks, and they certainly produce some knowledge for the core [knowledge], but I don't think they actively realise that this is the core of our knowledge.*

> ***P5*** *H1: By definition, all knowledge and information is considered 'company confidential'. Because publishing information in a publicly traded company is controlled, we need to have this basic rule that all information and knowledge is confidential.*

> ***P6*** *I: Who recognises [knowledge] as valuable?*
> *H1: The one who needs it.*
> *H2: It is spread out over numerous places in the company, so it should be recognised by the maintenance worker who works at the customer site; they should recognise what is valuable to the customer. But we have built a procedure for this in a way […], but it is bits from here and there. All knowledge from the customer interface is important.*
> *H1: But [the value of knowledge] is subjective and depends on the needs.*
> *[…]*
> *I: If you think about the individual maintenance worker or a salesperson, do they know what is valuable knowledge from the perspective of management?*
> *H2: Not always, but some know more. It is pretty much dependent on the individual. But what they do […] may consider our product or the product*

of the competitors, and little things within the customer interface. It comes from many directions, but we try to gather the essential part of it.

Knowledge recognition as depicted in these excerpts is a process of individual-level and collective evaluation. The importance of knowledge is not always self-evident; hence, there needs to be discussion of what knowledge is important to the company and what the company should do with it. Two additional perspectives can be pointed out from these extracts: first companies are talking about recognition of what knowledge is still needed. That knowledge does not necessarily exist yet in the company, or it might be available elsewhere in the organisation. This situation calls for active acquisition of the necessary knowledge. The other perspective involves recognition of the importance of existing knowledge. This perspective comes closer to the individual, who should be able to decide whether a piece of knowledge is valuable and judge how to treat it.

The interviewees stated that the employees do not always consider their knowledge especially important from the point of view of the company. The knowledge they apply to conduct their daily routines is just that to them: routine. Greater awareness of the importance of their knowledge to the company might change the way in which these people treat that knowledge.

5.2.3 Threats to knowledge

The interviewees were asked about what kinds of threats they feel exist to the important knowledge of their company. The threats are presented below and discussed with the aid of excerpts. The categories of threat are not mutually exclusive. In fact, there are strong links between them; accordingly, an extract may have been placed into more than one category. The categories are listed in Table 19.

Table 19: Categorisation of threats to knowledge

Categories of threats to knowledge	Explanation	Instances
Employee turnover	Employees who are leaving pose a threat to knowledge: when employees leave, their knowledge is no longer available to the company; on the other hand, too little turnover may pose its own threat to knowledge	6
Leaks of knowledge to competitors	Knowledge may end up with a competitor through their active acquisition efforts, and because of mistakes within the company	7
Intentional harm	Knowledge is leaked to outside the company because an employee chooses to act against regulations or, if there are no explicit rules in place, chooses not to follow proper ethics	3
Obsolete knowledge	Knowledge becomes obsolete if it is not actively updated and renewed	3

In the following discussion, each sub-category of threats to knowledge that is listed in Table 19 is discussed in more detail. The interviews show different approaches to why a certain element is a threat to knowledge and to how that threat is present in the business. Although the reasons may vary greatly from one threat to the next, the categories were not broken down further, as that would have led to a situation wherein a category was established on the basis of just one interview. Because the purpose of this content analysis process is to find themes that recur across the interviews, the categorisation was kept to a level at which each category was informed by material from at least two companies.

Employee turnover

The first threat that most of the interviewees mentioned was employee turnover. In this they were referring especially to employees leaving, which usually involves the arrival of new employees to replace those departing. This turnover can have many reasons – for example, discontent.

> ***P1*** *H1: There is a threat that knowledge will leave the company. Although people do stay quite well, some leave; there can be controversies, and very important knowledge can leave. As has happened to us. Internally we have this knowledge management threat. We don't have a solid chain of supervisors who would think about knowledge. We have a project organisation, and the project manager does not necessarily think about the knowledge from the development point of view as much as from the user point of view.*

This interviewee acknowledged that there can be difficulties with the roles of the employees and their supervisors. If the employees are not happy with the way the project organisation wants to use their knowledge, they may want to work for another company. In this case, the threat of losing important knowledge is caused by inadequate or bad management practices. Controversies caused by unreasonable management practices can be avoided by, for example, involving people in the planning of the work processes.

Another cause for employee turnover is sudden loss of personnel for any other reason. If people are taken for granted, the company can find itself in a difficult situation if someone important is lost. This threat can sometimes be difficult to recognise, since those who are taken for granted are just that – taken for granted.

> ***P2*** *H3: We do have this observation. One very experienced designer died. We have missed the knowledge that he had. At least you realise [the value] when you don't have [the knowledge] anymore.*

The knowledge of an experienced worker can prove essential, for a large amount of hidden knowledge lies in the experience that has accumulated over time. A company may recognise this only when it is too late, as in the case of company P2. If this experience is not replicated over time, it will end up lost when, for whatever reason, the person in question is no longer working for the company.

> ***P3*** *H2: Well, we have at least the threat that our chain of knowledge is very thin. We have a long chain, and a long part of it is formed of single knowledge-holders, or the key knowledge is possessed by one person. It's partly in our culture, but partly it has been caused by the 2008 recession. We have prioritised survival over having a reserve. But if we don't manage to duplicate [the knowledge of] those critical people quickly, they will burn out, leave, or become bottlenecks.*

In circumstances such as those of company P3, with its many single-person links in a chain of experts, it is not only turnover that constitutes a threat. Overworking these people is a threat, one that can, in its turn, lead to turnover. The company faces the challenge of transferring important knowledge to newcomers, to double the thickness of the chain, as it were, as the company works to increase its production volumes.

Employee turnover is not just a threat to knowledge, though. It can also be a positive thing, especially if the people decide to return someday. Turnover also brings fresh knowledge to the company, since the people who leave often need to be replaced with new employees. The threat of having to invest in training someone new may be balanced out by new knowledge and insight brought by that new person. Also, someone who returns to a company brings back new experiences of the environment, while still carrying the previous experience of working for the company.

> ***P4*** *H1: Of course, you might be upset at someone [leaving]: you wish you could have offered a suitable job for the person, but we are, after all, a small company. We cannot offer everything for everyone. In a way, we must see it as a healthy phenomenon that people also leave. And, actually, quite a few come back. I could instantly name five who have come back.*

> ***P6*** *H2: We had this one good fellow who left, so we told him: 'Go ahead, leave, and come back. Go practise at somebody else's expense for a while.' [The employee turnover is] not only a bad thing.*

The companies have experienced people leaving and then coming back with experience of different environments. Job-hopping is not as common in Finland as in some other countries, so companies can have greater confidence when encouraging some people to move on and maybe someday come back with new and potentially valuable experiences.

As the discussion above indicates, if employee turnover can be seen as a major threat to knowledge, lack of turnover too can prove a threat. If the same person is responsible for certain activities for years on end, a disaster can ensue when he or she eventually retires. Accumulation of knowledge in only one person over the years can lead to increasing risks when eventually the instance of turnover takes place.

> ***P1*** *H2: There is actually only one person who knows all our customers and how to do business with them, and the customer entity. And now when this person is going to retire, we have established this sort of master–apprentice setting to approach this problem. The apprentice will follow along for almost a year. And this is done solely because of the knowledge. On account of the person who is retiring, I don't think there is a single document about what he has been doing for the past [few] years.*

> ***P1*** *H2: There is this thing called the half-life of a manager. In five years, their efficiency will halve. In five years, they get stuck in routines and stop creating new things. So it is also not good to have one person in the same position as long as possible and in that way be efficient.*

In combination with a culture of non-existent documentation, lack of turnover is a real challenge from the standpoint of keeping knowledge available to the company. One approach to resolving this situation is a very long period of co-working by the employee who is leaving and the one taking over the duties. This enables knowledge transfer between people, but inevitably some documentation needs to be done also. Interestingly enough, the two above excerpts come from the same company, which tells of the approach to job rotation emerging in the company. If the philosophy of the second excerpt had been followed in the company for a long time, the problem described in the first one would not have emerged in the first place.

Knowledge leaks to competitors

Another threat that the interviewees recognised is espionage in its various forms. Competition brings with it the threat of competitors finding out about plans for the future, new products, pricing strategies, new customers, etc. The first form of this threat is related to turnover. Employees may end up working for a competitor when they leave the company. Especially in developing countries, the local companies are eager to hire people who have gained experience with a Western company.

> ***P3*** *H3: It is this mark of a Western company that they get if they have worked for us; they can cash in on it. For us, it is a source of leakage of process knowledge and product knowledge and other types. […] They have a growing market and a local government-owned company that would like to be over-aggressive in the market if it were possible.*

The Western companies organise their operations in ways that may not be familiar to more recent start-ups in developing countries, so the experience of working for a well-established company is frequently rewarded. Leakage of knowledge to competitors via turnover is observed to be an international problem. The companies assert that this is not a problem in Finland; instead, it is a problem in their offices abroad.

> ***P4*** *H1: Cultures are different. They do have a different attitude toward the employer in Asia, and when it comes to what is your own and what is not, there are different views on what is the right thing to do and what is not.*

Another interviewee spoke of this issue more directly:

> ***P7*** *H1: Well, we have challenges. There are different understandings of what is mine and not mine when you head eastward. You need to be careful with information security.*
> *I: What do you mean by that?*
> *H1: Well, it's tricky. We need to think that they are our employees and employees need to be treated equally. We cannot operate on the assumption that someone is going to steal or leak our knowledge, which, of course, from an information security point of view would be good, but not from the point of view of human relations. For example, in our office in India, where it is a known habit to bring data from the previous employer to the next one if you have the opportunity, it does bring you a headache. This is not so familiar for a Finn; we do have a more honest society.*

The interviewees claimed that employees in Asia are likely to take information and knowledge with them and give it to their next employer, most likely a competitor. This does lead to a question about whether employees in Finland really are more honest than those abroad or, instead, people generally tend to suspect foreigners of harming a company but not people belonging to their own ethnic group.

Also, one could turn the observation about the international operation environment on its head: If Finns tend to be honest, that may also mean that they are naïve. At least one pair of interviewees expressed a strong opinion about the Finnish mindset, which does not recognise threats to knowledge.

> ***P1*** *H1: We tend to be naïve, despite all [instructions]. Finland is still a very safe environment.*

This statement is supported by the common knowledge that in Finland it is normal to trust another person without questioning background, identity, or motivations. The threat of being spied upon is not perceived to be great. This, of course, does depend on the industry and the operation environment of the company.

> ***P5*** *H1: You could say that we work with an incorrect assumption that people understand what they should do.*
> *I: That's an interesting way to put it.*
> *H1: Well, I ground it in my knowledge that people don't know what they are doing. It has been shown and experienced many times. That's how it is. But it still is not necessarily [a bad] assumption; it is a manifestation of trust. Then we just have to be prepared to handle the cases, marginal ones hopefully, in which something does go wrong.*

Leaks of knowledge to competitors may be caused by naïveté of an employee or by just making a mistake or not knowing what one is supposed to do. Mistakes made at critical points can lead to results such as leaks. The interviewee quoted above stated that the company gives instructions and, in a way, operates with the expectation that people will follow the instructions. At the same time, they prepare for the scenario of something going wrong and knowledge being leaked or lost.

The threat of leaking knowledge to competitors was discussed by the interviewees also from the angle of intentional harm done by an employee who continues to work for the company. This links the two categories of threat closely together. Intentional harm may lead to information leaking but can also result in other security problems. This is why it is discussed as a separate threat category in this study.

Intentional harm

A major threat to knowledge that the companies recognised in the interviews is that of intentional harm done by an employee. This is a threat all companies need to acknowledge but cannot do much about. A company cannot operate on the expectation that someone internal could damage the company somehow, as previous excerpts have illustrated well. It could not operate sensibly on that expectation, since doing so would prevent people from doing their jobs. This is why this threat gets acknowledged, but there is little the companies examined have done to prevent it.

> ***P4*** *H1: But we do have this biggest threat: that somebody from inside our company would, for some reason or another, want to do damage. Because people always have access to knowledge if they work for us, and they should […], it is a single person in a critical place and discontented enough who can do the most damage. And it is a scenario that you can easily imagine. And in that situation there is not much weight on the contracts we have made that dictate sanctions if something bad really does happen.*

> ***P7*** *H1: Then, of course, there are these intentional information leaks. Luckily, we have not had them.*
> *I: What do you mean by an intentional information leak?*

> *H1: I mean that someone would intentionally take information away [and give it to someone else].*

These quotes also show that in the case of intentional harm there is little difference between leaking information and leaking knowledge. Whether the information or knowledge is leaked from information systems or by an employee, there is very little the company can do to prevent the leak. The company can only try to keep people content, such that they would not want to do harm.

Hoarding of knowledge by employees can be another cause of intentional harm. While they may not think of it that way, they sometimes intentionally hoard knowledge to improve their position in the internal employment market of the company. This is another aspect of the threat of too much knowledge being concentrated in one person – in this case, that accumulation having been caused in part by the person in question.

> ***P7*** *H1: On the other hand, there is a threat to knowledge in people hoarding knowledge for themselves. There is a trend of trying to get rid of that, because it used to be a problem that people would hoard knowledge and [thereby] be more important than others. We try to encourage getting away from that. How well this will work time will show, but at least we are encouraging it.*

If someone feels that he or she gains an advantage at the company by hoarding knowledge, hoarding is almost certain to follow. The company needs to find a way of eliminating that advantage in order to motivate people to share knowledge. The knowledge management initiatives in many companies are aimed at encouraging knowledge sharing so that hoarding of knowledge would not be rewarding for employees. Hoarding knowledge can readily result in inefficiencies and knowledge barriers within the company. As can be seen from the quote above, the results of a knowledge management programme are not visible instantly. They are reached with time, and many factors affect the outcome.

Obsolete knowledge

Another threat to company knowledge is that of outdatedness. If a company does not put active effort into developing and renewing its knowledge, the knowledge is going to lose its value. There also must be ability to recognise valuable knowledge at the time when it is valuable.

> ***P1*** *H1: [One threat] is knowledge becoming obsolete. If people stay […] I mean when we can recruit new people as we do now, we get new people and new knowledge. But the people we have inside are not all actively trying to learn new things. Of course, we do make education plans and 'force' people to renew [their skills], but there always is someone who gets left behind. I do see it as a threat that knowledge becomes old,*

because in our industry development is very fast. So the level of knowledge does not remain as high as it could be.

P2 *H3: Knowledge has value, and it depends also on the time. If there is valuable knowledge but it is not utilised, it will lose its significance.*

When knowledge has become outdated, it no longer has significance for the company. One challenge companies face is that of recognising the potential of their knowledge while that knowledge can really make a difference to the company. Over time, the knowledge may become common industry knowledge, at which point it no longer provides the company with a competitive edge. If knowledge is not utilised in time, it becomes less important for the company, because it is not unique anymore.

Companies find active renewal of knowledge to be desirable, both from the perspective of having active employees who want to learn new things and in terms of having the latest knowledge from outside the company at their disposal.

P7 *H1: [T]hat knowledge or information as such would become obsolete – that in a way is a threat, but, to my understanding, the people do update it, and we put active effort into this on the firm level too […]. But, of course, when the staff age, knowledge becomes obsolete. How to transfer knowledge is a problem. In the last couple of weeks, we have tried to transfer knowledge about my next [role], but it's not as if you could transfer it by connecting the heads of two people with a wire.*

Knowledge can become outdated if people become bogged down in routines, but the flip side of this threat is that knowledge does not get transferred when people switch tasks inside the company. Someone who is leaving a role is already putting effort into learning about his or her new role, and if there is not enough time for the transition, important knowledge about processes and, for example, product history or customer relations can go undetected. In these cases, however, it is usually still possible to access the knowledge, by contacting the people who used to handle the job in question.

P6 *H1: Then there are these border zones [between roles] that are at least as important [as the core tasks of roles]. I just had a good conversation today related to problems of the role change of one person. There is this basic assumption that involves something […] (a full-time job), and then there are the jobs of three people in the same area that come with it, because the person happens to know about these on account of job history, not because of the current role.*
H2: Roles are built on the basis of tacit knowledge.
H1: Yes, and I've always said that we have a very strong shadow organisation that we need to get rid of.
H2: Somehow we need to make that knowledge common.

In this case, the threat could arise also that the knowledge does not get transferred to the people who would actually need it and that people instead present their questions to people who no longer are officially responsible for a certain task. Their knowledge about the current situation may be incomplete, and use and propagation of obsolete knowledge can result while relevant knowledge is not transferred to the right people.

The main threats to knowledge highlighted in the empirical material are employee turnover, knowledge leaks, intentional harm, and obsolete knowledge. The interviewees identified other threats too, but most of their viewpoints could be categorised as related to sub-threats under these four. In the next section, the other side of threats – the protection mechanisms – will be discussed. An interesting point raised in the interview material is that the protection mechanisms the companies have in place are not entirely triggered by the threats identified in the interviews. They may correspond to the threats, but the motivation for applying them may differ from the actual threats.

5.2.4 Knowledge protection mechanisms

When asked about knowledge protection mechanisms, the interviewees did not mention many. However, some mechanisms were brought up when the interviewees were asked how their company protects against the threats to knowledge that they have recognised. The discussions in the interviews also revealed some protection mechanisms that the companies employed but might not necessarily have considered to consist of protection. The protection mechanisms found in the interview data are listed in Table 20.

Table 20: Knowledge protection mechanisms

Category of knowledge protection mechanism	Category definition	Instances
Information security policies and handbooks	Information security policies or handbooks are established in the companies to guide employees; these address not only information but also, at least indirectly, knowledge	4
Information security training	The employees are given information security training, which also addresses knowledge	7
Human relations management and knowledge management	Human relations management or knowledge management efforts are in place to counter, for example, threats linked to employee turnover or obsolete knowledge	7
Culture	The organisational culture of the company is used either consciously or unconsciously to direct employee actions toward important knowledge	4

The knowledge protection mechanisms listed in Table 20 and discussed below are very different in the approaches they manifest. Information security policies and training, along with human relations activities, can be highly structured and formal procedures at

a company. At the same time, the culture of the organisation is an underlying structure, not consciously and explicitly defined by the company. The interviewees may not have directly stated that they consciously use knowledge management processes to protect their knowledge, but when one analyses the threats pinpointed in the previous section, these practices can be seen as one solution for handling the recognised threats.

Information security policies and handbooks

The first mechanisms discussed were the formal information security policies. All of the companies had an information security policy, but it and the related instructions addressed mainly technical security measures. Discussion of how the instructions address other than technical security measures differed from company to company. The aim of the questions was to find out whether the policies address secure behaviour, non-technical threats, or other issues that are not directly technology-related. The first category in the policy discussion is represented by the extract below: the analogy between systems security behaviour and non-technical security.

> ***P2*** *H2: Yes, we do have an information security policy that addresses how to use our information systems securely. But it is mostly routine things, how to circulate information inside the company, what not to send outside, how to handle directories and databases, how to get to documents.*
> *[…]*
> *H2: [A]t least I think that this guides [people] also outside the systems. Maybe we have the opposite kind of problem – this is a personal opinion, but I feel that knowledge is shared also when not necessary. It sort of gives an 'is this really relevant [for me]?' feeling.*
> *H1: There is this [sense] that people should have enough understanding and wisdom, and behind those a lot of knowledge, that they can judge that this knowledge is sensitive and on these grounds. And a person in the outside 'circle' who is just curious, without any malicious intent, they cannot judge correctly, because there is not enough understanding.*

The information security policy is a document that communicates the need to protect information. How the policy applies to knowledge may be left to the interpretation of the interpreter. In the excerpt above, the manager states that the information security policy gives instructions about other behaviour than just actions that involve information systems. However, this conclusion appears to be drawn from an analogy rather than explicit instructions in behaviour. As the interviewee put it, 'I think that this guides also outside the systems'. Thus it is assumed that the employees are able to carry over the information-systems-related instructions to other activities.

In the interview extract above, the interviewees also say that not all employees have the ability to understand when knowledge needs to be shared and when the knowledge is not relevant or sharing is not desired. The instructions seems to leave a lot of room for

interpretation, and this, in combination with insufficient understanding of how to apply the instructions, can lead to problems in the company. The problem described by interviewee H2 is that people share information and knowledge that is not relevant for the task at hand. While this is not a big problem from a security point of view, the misunderstanding of instructions can lead also to more serious problems if the security level is reduced because of lack of understanding of the importance of knowledge.

The information security policy as a document may be important from the legal perspective or from a customer's standpoint, but in practice that document is often not very 'visible' to the employees. The interviewees with one company did acknowledge that communication about the information security policy may have been inadequate.

> ***P6*** *H2: We have quite a lot of information-security-related instructions in Notes: what to do, about passwords, and then, on the other hand, it is handled with the (outsourcing) contracts what they can do. But if you asked people about the instructions, it might be that many of them don't even know where to find them.*
> *H1: They'll roll their eyes.*
> *H2: Or ask: 'Do we really have these?'*

Lack of understanding of the content of the policy may stem from the fact that not all personnel are aware of the policy in the first place. One approach to communicating the information security policy is, instead of encouraging people to read the policy itself, to encourage them to read the documentation that explains the policy and brings matters down to a more practical level.

> ***P7*** *H1: We have a service section for information security on our intranet, and there is, beginning with the policy, a handbook that explains the policy. I wanted the policy to be as brief as possible. The meaning of the policy is to show the commitment of the management: this is what we do. The handbook explains the policy and gives practical instructions. It is a summary of all our information security instructions. So if something is not clear from the handbook, then there are more detailed instructions available on the same site. Mostly it is non-technical, less technical; the technical stuff is separate. We do have technical specifications, and I have made a sort of information security standard that explains our technical solutions. But that is not commonly available. It is restricted to those who [need it].*

The information security policy was clearly noticed within the companies as an important tool. In day-to-day work, however, the more detailed instructions referred to as a handbook or the like are the tools that are used, rather than the policy itself. The employees are not necessarily even aware that the company has an information security policy in place. Some of the companies were attempting to change this situation by means of training.

According to the literature, the information security policy should be updated regularly – for example, in three-year cycles. The problem with outdated policies is that they are no longer relevant for the company's operations. If the policy is not up to date, it does not end up guiding operations and the operations will dictate the policy. Keeping policies up to date can, however, be sacrificed for completion of more urgent tasks.

> ***P3*** *H4: Yes, we do have [an information security policy], but it has become outdated; let's put it that way. It would need updating. It is a paper collection of six different documents. And that's not all; it is in Finnish. We would need it in English, but, as [we've] said, we've been busy [with other things].*
> *[…]*
> *H2: This shows our situation. I'm relatively new here, and from my perspective most of the documentation is from 2007; some may be from 2008. After that, we have focused on survival.*

The information security policy document needs to be updated in line with the changes that occur in the company over time. At some companies, the passing of three years does not yet mean that the policy has become outdated. In the case of the above extract, however, 3–4 years of not prioritising the updating of the documentation had left the information security policy severely outdated and this had already caused some difficulties in operations. The company did realise that the documentation needs to be updated and written in appropriate language if it is to be useful.

> ***P4*** *H1: [Information security policies] were put on paper quite early. I remember creating some papers [in] 2002. So quite early on, we needed to decide things – for example, backup routines and some practical things got documented when we communicated them. You could say that in 2005 we had things even better covered, because they were clearly distributed in a smaller organisation. Now there is much more uncertainty about offices and all. I mean the document in itself doesn't do much.*

The introductory study shows that the smaller companies saw no need for information security policies, since they had a small number of employees. In the above quote, this perspective is challenged: when it was smaller, the company had all of the information security instructions documented and felt that they had everything well under control. With expansion, the situation changed, even though the documentation was updated. It is clear that a larger organisation needs to put effort into creating documentation that complements the information security policy. By definition, the policy document is quite short, so it cannot cover everything associated with information security practices and responsibilities. Information security handbooks that explain the policy are needed for clarification of the policy's message, because, for example, the policy could be interpreted differently in different locations. The more detailed instructions clarify what the policy concretely means.

At some companies, the information security instructions address primarily the use of information systems and the technical challenges of security. One company, however, stated that the instructions are prepared to guide behaviour in a broader sense than just guiding the way people act as users of the systems. The technical side of things at this company is still very important and has a big role, but the instructions are written from the standpoint of what is expected of the employees in terms of general behaviour.

> ***P5*** *H1: Actually, the information security instructions are not targeted at information or data systems. They are about information security in the broad sense, such as how the whiteboard should look after a meeting, and here [we have a blank board]. It's like this, but we have very little physical material in comparison to the quantity of data we have: we have a significant number of terabytes of data. So if you think about information security instructions, they mostly instruct in the use of information systems.*

Change constantly has repercussions for information security policies and instructions, yet, as we saw above, some companies stated that the instructions became outdated since efforts to update them had not been prioritised. Information security policies and instructions are seldom listed among the highest priorities, because that documentation is rarely needed at the customer interface. When the company's customers want detailed information about the information security policies and procedures, the documentation is updated more promptly.

> ***P1*** *I: Have these [information security] instructions or procedures changed lately?*
> *H1: Yes, they have changed; we had to develop new information security procedures, a whole new world here. The initiative came from our customers' demands. When the customers change their requirements, we need to react.*
> *I: Do they audit you?*
> *H1: Yes, and we carry out internal audits too.*

This excerpt implies that information security can be accorded a very high spot on the list of a company's priorities if it is demanded by the customers. Customers with high security criteria will get what they ask for. This should not be surprising, since no company wants to lose business on account of poor documentation of security practices.

The discussion on information security policies reveals that, while companies may have information security policies and instructions, not all of the participating companies are actively using these as mechanisms for protection of information and knowledge. The main reason for documenting the policies seems to be to satisfy technical security requirements. The policies address behaviour and handling of knowledge to some extent, but employees may not be aware of the policy, and, therefore, the role of the

policies as actual knowledge protection mechanisms is debatable. To reap benefits from the policies, the companies would need to set up training programmes to promote awareness of information security issues and the related policies and instructions.

Information security training

According to the literature, an information security policy coupled with proper training addressing the contents of the policy is essential to the information security management toolbox (von Solms & von Solms 2004a, Crossler & Bélanger 2009, Kayworth & Whitten 2010). The analogy between information security management and knowledge security would suggest that training holds an important role. The section above on information security policies shows that these policies are not used very actively to protect knowledge. The interviewees were asked about how the employees are trained on information security issues. Even if knowledge is not thoroughly addressed in the information security policies and instructions, there is a great deal that can be covered in such training, and, in fact, the companies were giving training on information security issues, even though the discussion on information security policies suggests otherwise. The forms of training and the approaches differ between companies.

> ***P5*** *H1: [F]or example, our training of new employees. If I give an example that you are a reporter and want to know what is going on at our company, what would you do? And the example I give is that you would go to lunch. Many of our people go to the nearby restaurants for lunch. And you would go there and listen. And this is why I have instructed to talk – technically speaking, it is your free time – talk about your hobbies, men, women, anything, but do not discuss work there.*

This example describes quite well the kind of training the company provides. With examples of expected behaviour and examples of what can happen if the desired manner of behaviour is not followed, the company gives a strong message to the employees. When a company is based at a busy business park or in another cluster of business premises, discussing work outside the office can lead to knowledge reaching the wrong ears.

In addition to dealing with passive threats, such as someone listening to conversations, training can cover active threats, such as social engineering. Defined as the exploiting of people's goodwill to gain pieces of knowledge that are confidential, social engineering is a threat that targets knowledge in particular. In that sense, it is interesting that social engineering was not mentioned as a threat in the interviews when the interviewees were asked what kinds of threats they protect knowledge against. Social engineering was mentioned only in connection with training, as an example of the kinds of topics the company's training covers. This means that social engineering, while seen as a threat in practice, was not high on the list of threats by priority. Social engineering is easy to cover as a training topic even if the companies consider it only a minor threat.

> ***P1*** *H1: For example, we train people to counter social engineering. Also, we discuss how to behave at fairs, what kinds of situations can arise, or, for example, at a bar […]. And of information security issues in the top 10, [one example is] naiveté, what that means in different situations.*

Training that deals with social engineering and communication situations addresses the goodwill that many people show. Many knowledge leaks have occurred because people want to help others or impress them. This is the kind of thing companies want to prevent, so training looks at appropriate behaviour in various communication situations.

> ***P6*** *H1: There are human-related issues, what we say and where, and where to use our laptops and when to use the screen covers, and that aeroplanes are the best place for industrial espionage.*
> *H2: I have read strategies of many companies [while on an aeroplane].*
> *H1: Not to mention heated discussions.*
> *H2: That is a big risk. Finns, especially engineers, don't need to be encouraged much to tell you how good their products are, and they willingly tell you a lot. That's how they are; they want to tell how great the things they have done are.*
> *I: Is there an instruction 'don't do this'?*
> *H2: Well, I don't know about an instruction, but let's say that-*
> *H1: 'Think about what you talk about and where you do it.'*

The training is aimed at increasing the awareness of what might be of interest to other companies or other parties. This is important for security of that knowledge. People need to know which locations are dangerous and where they can safely discuss work-related issues. Working lunches are common in many places, but having a working lunch at a public restaurant might not be a good idea. Another issue that needs to be taken into account is social engineering: people may not just eavesdrop on interesting talk; they might also ask directly for information and pieces of knowledge. In such situations, it is necessary to recognise that giving away even small bits of knowledge can be harmful, since building a big picture from many small bits is often the goal of social engineering efforts.

In addition to social engineering and other communication situations, the companies' training addressed topics such as secure use of information systems and proper behaviour in the office. Some kind of training at the beginning of employment was offered at most of the companies. This is in line with the observations from the introductory empirical study, according to which security training is offered mostly for new employees. This implies that the training is one way to introduce the employees to the processes and work habits of the company.

> ***P7*** *H1: We always give orientation training to new employees, and information security is one part of it. Then we have a Web course on*

> *information security; they are all quite basic. Then I go around and give talks at department meetings and such, and we have instructions on the intranet. In the [training], we have these common [themes of] what to watch out for and how to behave. Don't do this and that. And then, of course, there are technical issues, a superficial presentation of what we do on the technological level. And I always emphasise what people should not do even if we have these technology instructions in place.*

Although the contents of information security training and the training format vary from company to company, training was seen as essential in all of the companies. The training sessions did not cover only technical issues of how to use equipment and to save data. Security-friendly behaviour and attitudes were addressed by most companies participating. However, a question could be raised as to what the interviewees meant when speaking of non-technical issues. Some interviewees did mention behaviour and awareness as non-technical security issues, but others cited even employees' habits in use of technical equipment as a non-technical issue.

As for the frequency of training, some companies had a well-established information security training programme, and some acknowledged that they should offer more training. Information security training does not necessarily need to involve separate sessions; it might be a good idea to embed it in other training. At the same time, always pairing information security with IT training perpetuates the common attitude that information security is only related to the use of information technology.

> ***P4*** *H1: We have this employee handbook, which contains, in principle, everything you need to know when you come to work for us, and it [information security] forms one section of it. And all employees will get information-security-oriented training in our IT systems. It's quite comprehensive, but the problem is that I'm not at all sure that all of our new employees in all countries receive the training; it's always the responsibility of the local office.*

The training programme at company P4 seems well-established and the contents of the training thought through well. The problem seems to be that expansion to new countries has brought an aspect of independence to branch offices. The manager here in Finland was not directly responsible for all training anymore, and he admitted that it is unclear whether all new employees actually receive the training as the head office intends.

The need for training at the companies has been judged on the basis of practical considerations. Lack of understanding or of proper knowledge of the instructions can cause problems that could be avoided by means of training about the secure practices. This practicality-paved route to training, which has probably been travelled by many of the companies, was directly discussed in one interview. Company P6 had recognised a need to establish training, and they had undertaken large-scale training efforts.

> ***P6*** *H1: A couple of years ago, we realised that this is a deficiency and went through everything with a big training round. And now we have these monthly ICT training sessions that have more to do with the user environment but that include also some information security issues.*

In summary, the companies studied were offering training in information security, and some interviewees stated that the training programmes target non-technological issues of information security, which in the context of this study can be positioned under the heading of knowledge security. Training is a way of complementing the information security policies and instructions, but, depending on the point of view of the person who plans the training, its focus can still be too much on information systems and their secure use. If the training is arranged by a technologically oriented person and knowledge security is no-one's responsibility, knowledge is only very vaguely considered in the training materials.

Human relations management and knowledge management

One notion supported by the interviews is that human relations practices form one driver of knowledge security. Through them, companies aim for lower or more controlled employee turnover, and thus tackle the threat that excessive turnover poses to the knowledge in a company. Another way in which human relations practices can protect knowledge is by keeping people content. Employees who are happy with their work conditions and salary are less likely to cause harm to their employer.

Knowledge management is practised by many companies, but not all of them apply actual knowledge management theories or call the activity by that name. These activities are intended to promote the proper use of knowledge assets, with the right people carrying out the right tasks and facing the right quantity of challenges.

> ***P4*** *I: Do you discuss choices about important knowledge in strategy meetings?*
> *H1: Yes, we do, but not with that name. For example, we want to develop our important employees, and these key personnel who have the important knowledge. We talk about how to keep them with us and how to motivate them and so on, and this way we do discuss it a lot. But we don't talk about knowledge management; we talk about managing people. So the terms [-] we don't use them actively, but we pay a lot of attention to these issues.*

The balance between keeping people content with their job and having adequate security measures in place is a challenge. Conflicts between these goals are unavoidable, and companies need to handle them. The issue is partly caused by management challenges of finding meaningful roles for all employees. Not all employees are content with many restrictions to what they may do and what knowledge they are permitted to access. On the other hand, not all employees are happy to share all

their knowledge with other employees such that the knowledge is secure for the use of the company in the event that the employee in question leaves. Knowledge management initiatives as a knowledge protection mechanism address both the threat of too much personnel turnover and the threat of too little. These goals themselves demonstrate that the knowledge management tasks focus on finding a good balance between the efforts.

Companies need to find their way of doing business by allowing enough access to information and knowledge while still limiting that access to a sensible minimum. And this needs to be done without flooding people with too much knowledge or upsetting them with too many restrictions.

> ***P4*** *H1: It is an eternal conflict [between knowledge sharing and security]. It would be nice if everyone could have access to everything and you would never have to ask for things from IT. But the world does not work like that; it's a constant balancing act. As I mentioned, we have had mergers; these have caused the biggest problems, because we have had to establish some Internet security culture in the merged companies. And that is an ugly and bureaucratic thing, but it is a must. There are a lot of examples of what happens if things are not done even nearly right; we simply cannot afford to slip there. We need to balance between how much to invest in hoarding information and keeping it secure versus having everything in the open, and somewhere in between is a middle ground that we try to cover.*

Limiting access to knowledge and guaranteeing confidentiality of knowledge is one aspect of making that knowledge secure. As can be seen from the above quote, finding a balance, a point where there is enough restriction yet enough openness, is a challenge in itself. However, that balancing is done mostly within the dimension of confidentiality. The next interviewee quoted reminds us that there are two other dimensions to information security: integrity and availability.

> ***P5*** *H1: There are three elements in information security: there is, of course, confidentiality, which means whether it is a problem if it [information] ends up in the wrong hands. But there are availability and integrity too. And now there is a small amount of information that needs to be kept in a small circle for a range of reasons. There may, for example, be a bunch of information that might cause considerable damage for a company or its customers if it landed in the wrong hands. But for a company I see availability as a bigger threat. The activity cycles in companies are faster and faster, and I feel that, for knowledge, the bigger threat is that it is not available, not that it would be too available.*

Availability of knowledge is essential in the dynamic environment of today's business. With the ever-increasing pace of change, even the absence of one person at a crucial time can slow a company down considerably. This is something that companies must

address. People possess knowledge and share that knowledge within the company. There are pieces of knowledge that companies need to place under strict control of confidentiality, but there is also much knowledge that needs to be available in time for the company to react to its changing environment.

One of the threats mentioned at the companies was that of knowledge becoming obsolete. Therefore, the companies' knowledge management initiatives need to take into account also the changing needs for knowledge and the constant change. It is not enough for people and their knowledge to be available to the company. The employees need to renew their knowledge all the time in order to keep up with the changing environment. By actively training its employees and sharing the knowledge, a company can acquire and create new knowledge that keeps it abreast of the rapid change surrounding it.

The protection mechanisms employed to counter threats to knowledge can be various. The case companies tried to instruct their employees actively in secure behaviour and use practices. Policies, instructions, and training were in place to promote awareness of the threats, along with awareness of what information and knowledge is important to the company. Human relations practices too can be seen as protection, though a less conscious way of protecting knowledge. A side product of having employees who enjoy their jobs is that they pose less of a threat to the company and are likely to remain available to the company.

5.2.5 Culture

Culture was presented in Chapter 2's theory-oriented discussion as a major driver of knowledge security efforts, so the issue of culture was analysed also in this empirical study. In many of the interviews, either organisational culture was discussed directly or its impact on security measures was indirectly evident from the interviewees' answers. The direct discussions of organisational culture emphasise that it has a great impact on how people behave and what kinds of decisions they make.

Culture as an element that drives behaviour and people's decisions is the first aspect of culture that can be derived from the empirical material. The interviewees felt that every company has its own information security culture and that adapting to said culture takes time. Only some parts of a company's practices can be communicated by instructions given to the employees; the rest is communicated through the culture over time.

> ***P2*** *H2: I think I have gone through this in my earlier job, and now here, maybe on a different scale. But I think it [information security compliance] is the same in every company, and it is developed through the organisation's culture. You can instruct in what information [you can share], but you can't describe everything in instructions. There are always*

> *things that depend on your judgement, and the judgement depends on the culture and organisation you are in, and the boundaries that the organisation has set.*

Knowledge security is ultimately about individual people and their choices to share some piece of knowledge with other people. According to this interviewee, there is a limit to how much can be done via instructions, and the rest is determined by how well the organisational culture supports a person in making compliant choices. With this approach, employees' judgement is something that managers might need to think about more carefully. Could there be ways to influence the culture of the organisation consciously so that people would make the choices the company wants them to make?

> ***P6*** *H1: One threat [to knowledge] is [found in] how the organisation lives with producing and using of knowledge: is it iterative, is it directed from the top down or from the bottom up, and how does it [knowledge] move horizontally?*
> *H2: How it fits the culture and values and the usual way of working in the company. I think there is a lot of knowledge that is not utilised […]. We may not make the good choices because they diverge from the usual mindset.*

The context of the above extract is a discussion of whether the organisational culture of the company posed a threat to the utilisation of knowledge. If a company gets mired in traditional ways of doing things, it may rule out solutions that would be beneficial for the company in the future. The interviewees may be referring to the 'not invented here' syndrome that many companies suffer from: a new idea is discarded because it departs from the usual ways of operating at the company. This highlights the availability side of knowledge security: is knowledge readily available to all who need it? A challenge to availability can arise also when the knowledge could have been made available but was not recognised as valuable or is discarded because it comes from the 'wrong source'.

Another aspect of culture coming up in the extract is related to the phenomenon of the direction of knowledge flow reflecting the culture. A strongly hierarchical culture is seen in the literature as an inhibitor of knowledge flow from the bottom up in the organisation (De Long & Fahey 2000, Riege 2005). The above extract shows discussion of whether the knowledge moves mainly top-down or bottom-up, and also of how knowledge at the company flows horizontally. The discussion thus refers to whether the company's culture supports the flow of knowledge from the bottom upward enough and whether it also supports horizontal exchange of knowledge adequately. The climate at a company may have a strong influence on horizontal flow of knowledge. The next extract carries the discussion of organisational culture forward from the angle of company spirit.

> ***P3*** *H2: What about the spirit of our company? Do we use that to make our human capital secure? How do we use that as an instrument?*

> *H1: I would say that we do use it, but at the moment the spirit has gone through some tough times. I mean now we have a lot of people who are not as committed to us as before. When the company spirit was strong, people were really committed to this.*
> *H3: It was a community instrument, kind of a post-industrialist effort to raise spirits, a sense of unity or something like that. So thinking of structural capital, [I find that] the spirit has been one asset.*

A company with a strong sense of unity and shared efforts is a company that is likely to inspire its employees to commit to the goals of the company. Company P3 saw a strong group spirit as a way toward secure knowledge, in that it keeps employees motivated and committed. The interviewees stated that company spirit has been a very important instrument for them but that in times of crisis the spirit has suffered a lot, and they were not sure it can work for the benefit of the company in the new situation.

A very strong company spirit communicates a strong culture in which all employees, regardless of their position, are committed to the success of the company. If the company is not succeeding in the market and perhaps needs to let some employees go, it is evident that the spirit must suffer and that cultural unity is damaged. This is a very good example of the connection between organisational culture and climate: the climate reacts very rapidly to changes, and it reflects the slower cultural changes (see Subsection 4.3.2). If a spirit that once was very strong is dampened for a long while, the cultural dimensions of mutual goals and strong commitment to the company may suffer. This is a security issue not only because of the threat of losing important employees but also because unhappy and non-committed employees can cause security threats to the company (Whitman & Mattord 2003, ISO/IEC 2005, Kumar et al. 2008).

Situations of change create challenges for any company. For companies with a culture that embraces change as an opportunity rather than a threat, making changes may be easier; however, change nearly always brings some trouble with it.

> ***P4**: H1: Change [in security instructions] brings trouble because for some it is a huge demonstration of distrust if they don't have access to somewhere that they used to [because the growth changes the need for security]. People can take this very personally, and small and simple changes can grow into surprisingly big issues […]. So when we try to bring some information security culture into the company, the people who have been here a long time may not understand why the change is needed while people who are new take the instructions as a given.*

Changes in instructions and work procedures are among the changes that can affect companies' knowledge security. The growth of a company changes people's roles and also brings new ways of distributing responsibilities within the company. This may lead to situations wherein people find their access to certain information and knowledge more limited than it was before. In the case of company P4, this led to difficult

situations, with people reacting negatively to even small changes made for the sake of security.

Preparedness for change within an organisation is another factor in security associated with change. Employee turnover is among the threats to knowledge analysed in Subsection 5.2.2. This threat has a cultural dimension that is very well expressed by the next interviewee quoted:

> ***P6*** *H2: We acknowledged some time ago that we have 20 or so people who by leaving the company could close us down. The amount of tacit knowledge that they have accumulated over time is huge. Our culture has been such that you don't have to model everything. But now that we are growing and bringing in new employees, we cannot work like that anymore.*

The culture in company P6 has involved communicating many solutions and changes by means of discussion, and many solutions have been rolled out without modelling and documentation. The strong culture of face-to-face communication thus shown ended up creating problems from the standpoint of growth. The company realised that, because many solutions went undocumented, valuable knowledge was not being used to the company's greatest benefit. This threat had been addressed through the establishment of knowledge management practices aimed at better documentation and active communication and modelling of solutions.

On one hand, not communicating and not sharing knowledge is a threat to knowledge, while, on the other hand, sharing knowledge can be seen as a threat to the company. Companies must balance actively between sharing knowledge and spreading it, in order to increase awareness of it throughout the company and still actively protect knowledge from being shared too widely. This balance is difficult to reach and maintain.

> ***P1*** *H1: Developing knowledge and competencies is difficult, because we should develop on a wide scale, and then we have information security that limits it: you can't tell anything about this.*
> *H2: Information security is connected to the levels of technology, systems, and industry. Of course, we can share lower-level issues. But it is a big issue mentally also: we do things together, and then someone says you mustn't say anything. On one hand, we want everybody to know everything, and on the other there is a demand to shut up.*

A company's culture needs to reflect the information security instructions; otherwise, there will be problems. In the above extract, the interviewees describe the challenge of conflicting instructions: knowledge should be at the same time shared and not shared. The culture can have a key role in how this dilemma is solved. A culture that supports the security instructions supports reasonable knowledge sharing: knowledge is shared at the company to an extent that is beneficial to the operations but does not compromise

secrets. This requires deep understanding of the elements of knowledge as something that needs to be shared yet also has to be kept secret. A culture that, on the contrary, disregards the security instructions is going to encourage knowledge sharing despite the risks it can cause. Company P1 were moving toward a balance from the other end of the scale: knowledge was not being shared quite enough, and they were working toward a good understanding of what knowledge they should and could be sharing more widely within the company.

5.3 Summary of the empirical findings

The participating companies seem to have shown a fairly good understanding of what knowledge is important to them. Unlike in the introductory empirical material presented in Chapter 3, the companies here were asked specifically what knowledge (‘tietämys’ in Finnish) is important and valuable to them, and the general concept of information (‘tieto’ in Finnish was avoided . The companies’ most important knowledge is that forming the basis for their products; without the employees’ knowledge and understanding, the companies could not develop the products that they now produce.

A noteworthy finding is that the understanding of important knowledge was fairly similar across the case organisations, which operated in various industries. This supports a tentative generalisation that the knowledge of employees who contribute to the development and production of products is essential for companies, no matter what the product offering is. This conclusion is in line with the literature: knowledge is an essential resource for all companies (Wernerfelt 1984, Barney 1991, Grant 1996), no matter the industry.

If the observations from the introductory empirical material and the primary empirical material are considered together, the most important information for a company can be seen to be the information it receives from customers, and the most important knowledge is the knowledge used for processing of the customer information into products. The important knowledge is, in other words, about design and production, about the customers and their needs, and about the structures and organisation of the company. The interviews show that the managers at the participating companies were well aware of the value of knowledge for the company but were not sure whether all of the employees were aware of the value of their knowledge. The discussion of culture in the primary interviews also points out the challenges of managing how the valuable knowledge gets shared in the company, and with whom.

The characteristics for knowledge – integrity, availability, and confidentiality – were seldom addressed directly by the interviewees. The initial approach of the interviewees to the idea of valuable knowledge as being confidential was the only real discussion of the characteristics in the interviews in the primary empirical study. However, the threats to knowledge cited show that the threats recognised in the companies are not only

threats to confidentiality: employee turnover threatens the availability of knowledge also, and knowledge becoming obsolete is a threat to integrity. In this sense, all of the characteristics were present in the primary study's findings. The elements of people, process, and technology were all present in the discussions too. People were considered the holders of knowledge, and their knowledge of processes was deemed very important. Only the technological aspect of knowledge did not get a strong role in the interviews – since the focus was on knowledge that is bound to people. The various perspectives on knowledge seen in the primary empirical material are presented in Figure 33.

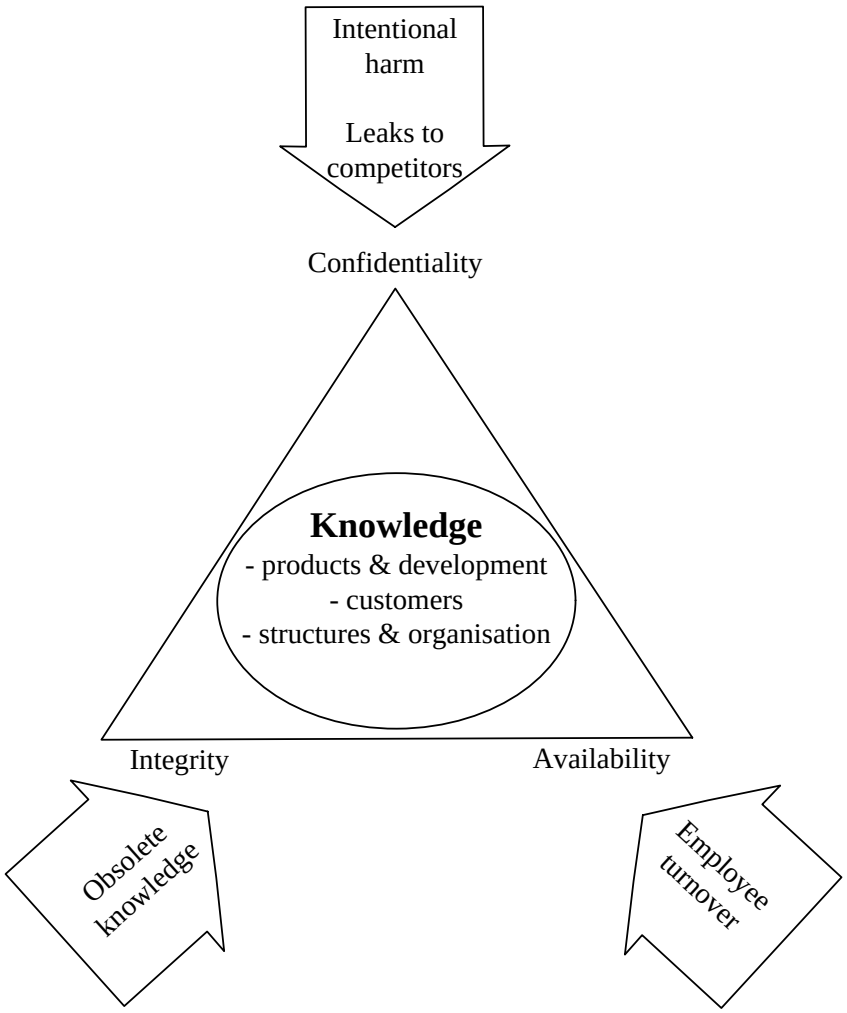

Figure 33: Threat-based perspectives on knowledge identified in the primary study

For the most part, the threats that were discussed in the interviews are considered to come from inside the company: too much or too little turnover, intentional harm done by employees, and obsolescence of knowledge. Knowledge leaks to competitors can be considered either an internal or an external threat, depending on the cause of the leak. Accordingly, the threats in Figure 33 are presented more from the perspectives of which characteristic they threaten than as internal threats or threats from outside. In the interviews, one fundamental source of information security threats, human error, did not

get a big role. People make mistakes and misjudgements, but these were likely considered more as a cause (for example, of knowledge leaks to competitors) than as a threat *per se*. In the case of knowledge, a simple mistake was not seen as a threat in the same way that entering information in the wrong place or using equipment in an incorrect way would be considered an information security threat.

The main threats to knowledge were considered to be connected to the operations of the company. Also described at company level, instead of the level of individuals' actions, were the protection mechanisms that the companies applied to counter these threats. The protection mechanisms identified from the primary study are illustrated in Figure 34.

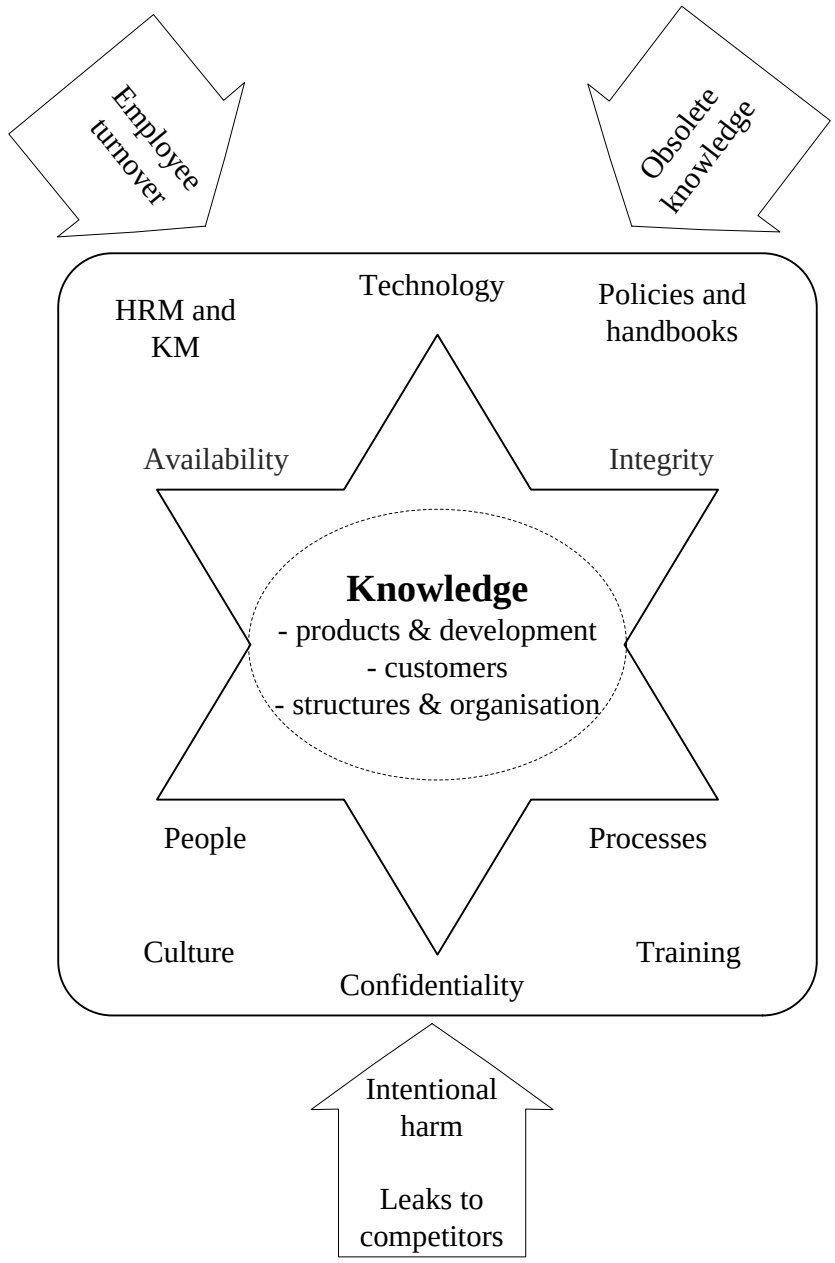

Figure 34: Protection mechanisms identified in the primary study

The first protection mechanism discussed in this work, information security policies and handbooks, is placed in the upper right-hand corner of Figure 34. Information security policies and instructions were used at the companies mainly to protect data and information. The interviewees stated that the policies and instructions address also non-technical issues of information security and, thereby, also knowledge. The policies and instructions contributed to knowledge security by instructing in secure behaviour and by clarifying the roles of the employees in connection with security. Although the orientation to information security was quite technical, the companies acknowledged that knowledge needs to be protected too, and that not all of the protection can be done by technical means.

In the lower right in Figure 34 is the knowledge protection mechanism of training. Information security training is a key mechanism for protecting information, but it can help protect knowledge also. The training topics described by the interviewees are very much connected to behaviour and judgement. Where knowledge is involved, people's appropriate judgement is an essential means of protection. The interviewees felt that employees may not always recognise their knowledge as valuable to the company. This raises the question of whether employees are able to make good protection decisions if they do not recognise the value of their knowledge.

Another mechanism that the companies were using to protect their knowledge is their knowledge management and human relation management practices, in the top left corner of Figure 34. The knowledge management initiatives in the companies were aimed at better availability of knowledge, wider sharing of knowledge, and better documentation of knowledge at the company. Although they would not call it knowledge security, the companies did strive for secure knowledge in many ways. Problems with turnover of employees had led the companies to realise that their employees possess a large amount of valuable knowledge, which should be utilised well in the company. One aspect of this is to keep it secure within the company – i.e., guarantee the confidentiality of the knowledge. Another element is keeping the knowledge secure for future use, ensuring its integrity and availability.

Many human relations management (HRM) activities at the companies were aimed at managing employee turnover such that there is enough but not too much of it. One aspect of HRM is that with careful consideration of competencies and the right meshing of personalities and communication styles, people are likely to be content in their jobs. Content employees want to remain at the company where they work, and they wish to see it succeed. It is clear, therefore, that HRM practices have a great deal to do with preventing knowledge security threats.

The organisational culture, in the bottom left corner of Figure 34, is seen in this study as both a way to protect knowledge and a potential cause of threats to knowledge. Culture has a large impact on how the training is carried forth into day-to-day operations and on how the employees respond to the training. If knowledge is considered a valuable asset

in the company and people get rewarded for protecting the knowledge assets in various ways, the company can create a culture that encourages knowledge security.

6 Conclusion and implications

This chapter presents a synthesis of the theoretical and empirical findings, along with the conclusions drawn from both sets of findings. That is, the final steps in Figure 8 (see p. 15), steps 10 and 11, are addressed here. The goal of the research project has been to find out what knowledge security is, with the definition of this concept being constructed from both a theoretical and an empirical study. After the final definition of knowledge security, the theoretical and practical implications of this concept are presented. At the end of the chapter, the study is critically evaluated and the results are discussed.

6.1 A definition for knowledge security

The triadic nature of a concept was discussed in Subsection 1.3.1: a concept is a combination of a term, one or more definitions for the term, and the phenomenon that the term and definition(s) describe (Niiniluoto 1984). As the research question posed for this study is what knowledge security is, the aim was to find a definition and a phenomenon that are connected to the term 'knowledge security'.

At the end of Chapter 4, knowledge security was defined as *the process of making and keeping the knowledge of people working at a company secure*. The process nature of knowledge security is evident from the theories constituting background for the work: security is a process aimed at reaching a secure state for a phenomenon. This process is an infinite effort, since a state of complete security is elusive and, in fact, illusory: because of constant change in the environment, it is impossible to reach. Knowledge too is a dynamic asset, in this creating another layer of change that security efforts must tackle.

The process nature of knowledge management and security management efforts was identified at the end of Chapter 2. Although the knowledge management processes presented in Chapter 2 are underlying influences on knowledge security, knowledge security as a process can be seen as an analogue from the information security management process. Therefore, the basis for the knowledge security process can be found in the security management processes. A knowledge security process constructed on the basis of the security management processes presented in Subsection 2.3.3 of this study is depicted in Figure 35.

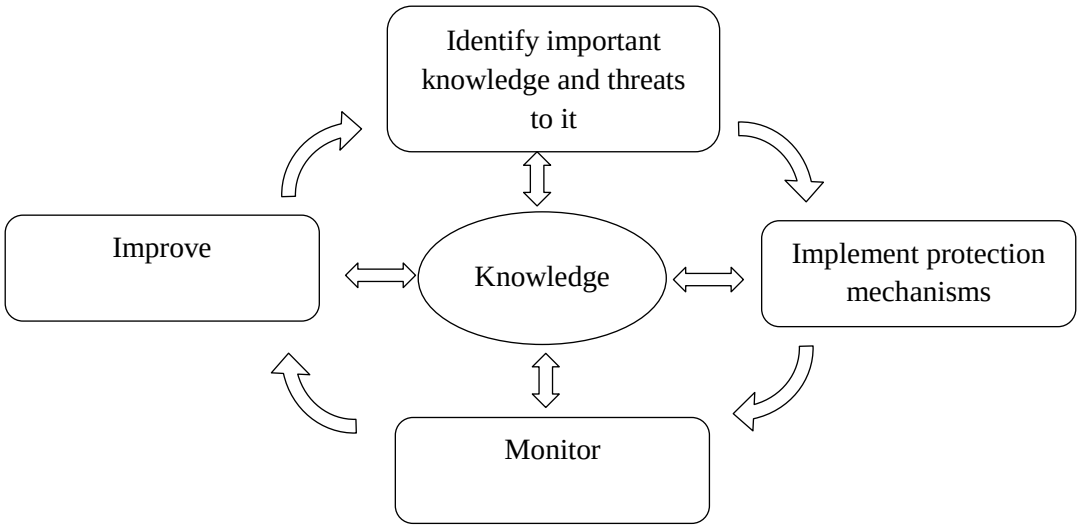

Figure 35: The knowledge security process

The theoretical and empirical discussion both bring up the perspective of threats to knowledge. By definition, security is the lack of threats, or the state of being safe from threats. Therefore, the first step in the process of knowledge security as presented in Figure 35 is to recognise the threats that important knowledge faces. For a company to be able to recognise the threats to its knowledge, it needs to recognise the important and valuable knowledge it possesses. Both the theoretical and the empirical material indicate that this is not always easy, and sometimes it may be that even if the management at a company know which knowledge is valuable to the company, this view does not hold throughout the company.

When a company has recognised its valuable knowledge assets and also communicated about this importance and value to the company, it can begin to identify threats to the knowledge. A framework for conceptualising the threats to knowledge, created on the basis of the theoretical and empirical study, is presented in Figure 36.

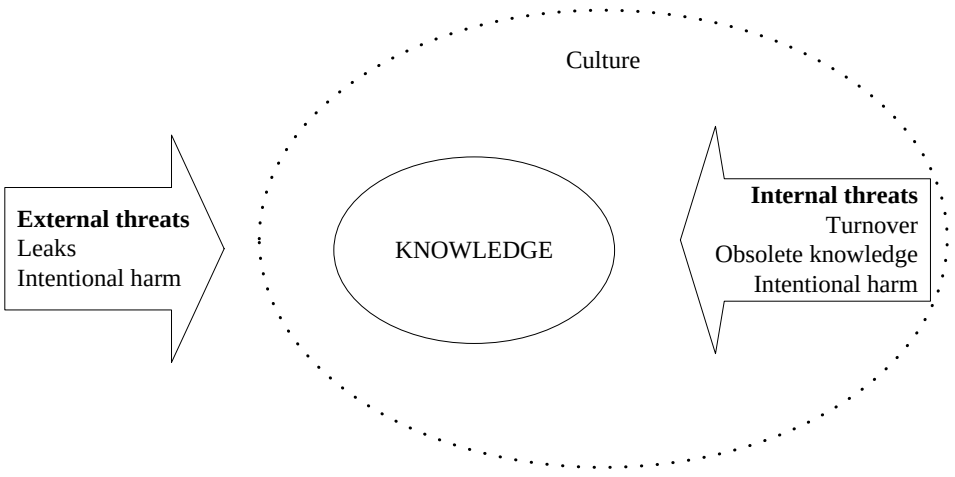

Figure 36: Threats to knowledge

In Figure 36, the main types of internal and external threats are presented. The primary threat to a company's knowledge from outside is the competitors of that company; they may be interested in many aspects of the company's business. For example, obtaining crucial pieces of knowledge about the company's plans could help competitors react earlier and thus narrow the competitive edge the company has over them (Helms et al. 2000). Competitors may be actively hunting for this knowledge, and this threat needs to be countered with good knowledge security practices such as careful compliance with the instructions not to discuss company-confidential issues in public places.

Even if they are a big threat, the competitors are not the biggest threat to knowledge revealed by the empirical material gathered for this study. The discussion of threats to knowledge concentrated on internal threats that the participating companies need to recognise and address from within. Employee turnover, obsolete knowledge, and knowledge leaks are threats originating inside the companies, so they cannot be tackled with simple solutions. Also, employee turnover is a threat that will always exist, so, instead of trying to avoid this threat, a company needs to plan for it. The other internal threats listed can be mitigated a bit more fully with solid knowledge security measures.

Once the important knowledge has been recognised and the threats to it are identified, the second step in the knowledge security process illustrated in Figure 35 is to choose and implement protection mechanisms. One way to approach the threats to knowledge is via analysis of the threats from the perspective of the characteristics for secure knowledge (confidentiality, integrity, and availability), which were introduced in Subsection 2.3.2. Figure 37 presents the characteristics in combination with solutions that address the threats presented in Figure 63. The perspective of the characteristics brings out dimensions of knowledge that managers may not always consider.

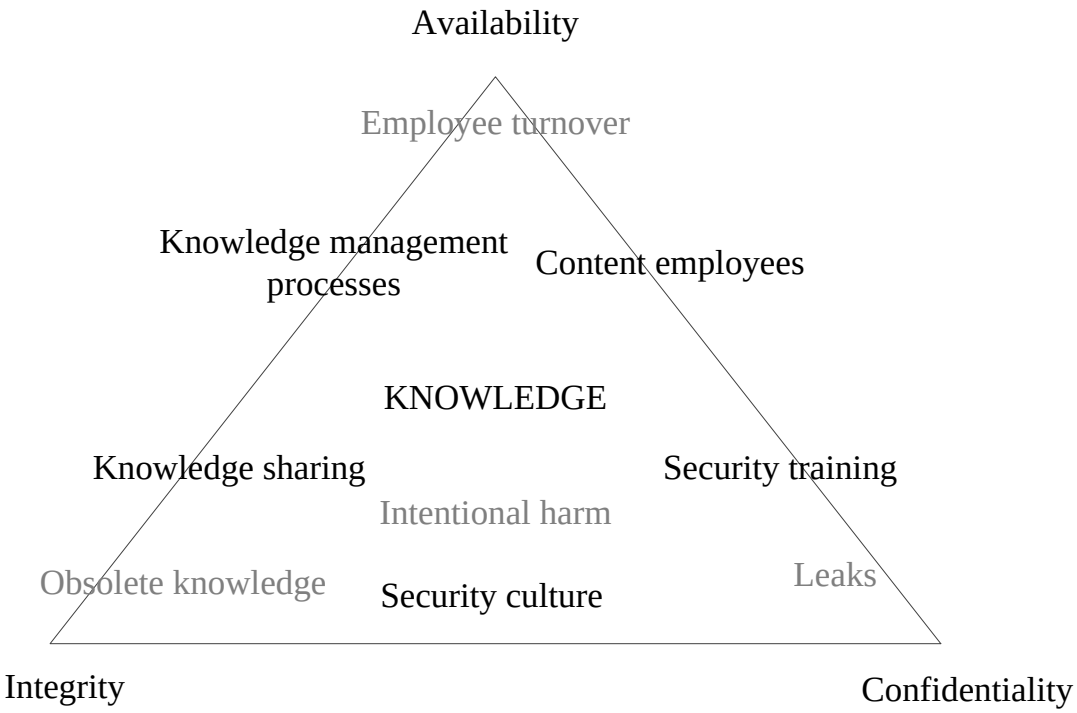

Figure 37: The CIA approach to security of knowledge

When threats to knowledge are examined, the confidentiality of knowledge seems to be quite well considered. In the context of information security, this is the characteristic that is addressed most by companies, as one can see from the introductory empirical material in this study. The confidentiality dimension of knowledge security is illustrated on the right-hand side in Figure 37. The solution of security training seems from the interviews reported upon in Chapter 5 to be thought of most often in terms of ensuring confidentiality of knowledge. The interviewees mentioned many examples of training topics that emphasise the confidentiality aspect of knowledge: the knowledge that is specific to the company and considered secret is not to be discussed in public places or with outsiders. Training could, however, also directly address topics such as why the availability of knowledge is important for the company or how the employees can update their knowledge and check its integrity and accuracy. These kinds of issues may have been covered to some extent in the training that the companies were already providing, but the interview material does not include discussion of training topics that are related specifically to the availability and integrity of knowledge.

In the empirical material, employee turnover is seen as a threat to knowledge that arises either through too much turnover or with too little turnover. Excessive turnover can threaten the availability of knowledge to the company, the dimension illustrated at the top of Figure 37. Keeping employees content by means of good human relations practices and reasonably challenging tasks is one way to protect the availability of knowledge and reduce unwanted turnover. Since turnover remains unavoidable, a company, while trying to reduce it, also needs to prepare for it. Knowledge management

systems for codifying knowledge and other knowledge management practices for sharing knowledge are needed, to reduce the impact of loss of employees.

When knowledge becomes obsolete, its integrity is threatened. This is illustrated on the left-hand side in Figure 37. Outdated knowledge can no longer be relied upon as beneficial for the company, so constant renewal of knowledge and creation of new knowledge must be sought at companies. Knowledge management initiatives address not only the availability of knowledge but also its integrity by encouraging employees to share their knowledge actively with each other. This spreads ideas and ensures that the ideas are tested and the knowledge updated by more than just one person. Constant interplay between tacit and explicit knowledge is a result of active knowledge sharing in a company. This also creates new knowledge for the company and through this is a good way to protect the integrity of that knowledge.

At the bottom in Figure 37, a good security culture is depicted as a way to ensure confidentiality and integrity of knowledge. As discussed in Chapter 5, the organisational culture can be both a threat to knowledge and a protection mechanism. By identifying threatening elements of the culture, such as excessively open communication or lack of attention to threats, a company can address them and guide the culture in a safer direction. The impact of the culture on the security efforts and the impact of the security efforts on the culture need to be acknowledged and a good culture nurtured. The various perspectives on culture identified in Subsection 2.4.5 can point to ways to address culture in the context of knowledge security. Knowledge security is by no means a separate activity from the everyday operations of a company. On the contrary, it should be embedded at the level of routines and people's assumptions. Before this point can be reached, conscious effort in implementation of protection mechanisms is needed.

One knowledge-management-focused approach to the threats to knowledge is to consider the dimensions of people, process, and technology. These dimensions and the main approaches to countering threats along them are illustrated in Figure 38. The 'people' dimension of knowledge management emphasises knowledge sharing and transfer of knowledge between individuals, both of which can be seen as one way to counter threats to knowledge. A company might eschew knowledge sharing efforts for reasons of security, and indeed security is an additional perspective that needs to be considered with knowledge management initiatives. Knowledge sharing may counter the threat of losing knowledge through employee turnover, yet excessive knowledge sharing could endanger important knowledge by revealing it to too many people. Therefore, balance needs to be found between sharing too little and sharing too much.

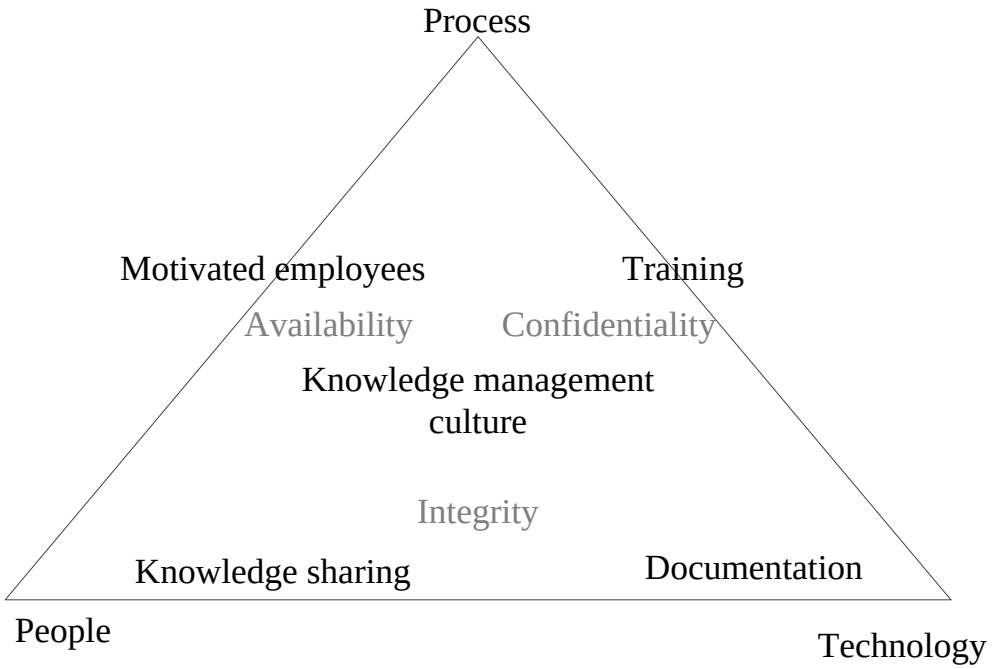

Figure 38: The knowledge management approach to security of knowledge

Another approach applied in knowledge management to loss of knowledge is documentation, found in the bottom right corner of Figure 38. This is an activity that supports knowledge sharing efforts. Here technology is considered a setting and target for knowledge transfer. Documentation cannot fully meet the need for security of knowledge: for example, not all knowledge can be codified and documented. However, it can act as a knowledge security process complementary to the knowledge sharing that takes place on the individual level.

The third dimension and site of knowledge illustrated in Figure 38 is processes. As the previous chapters have pointed out, knowledge management is very much manifested in various processes. The processes are also themselves a setting and source of knowledge. The process perspective may be applied also for considering all of the company's processes as knowledge processes that create and foster knowledge. The presence of motivated employees in Figure 38 is related to the threat of knowledge becoming obsolete or being lost in consequence of employee turnover. Motivated employees are likely to take a more positive stance toward new ideas and new knowledge. High motivation may also be one way to retain employees and prevent excessive turnover. Knowledge management processes may not be aimed directly at motivation of employees, but the results of, for example, systematic knowledge creation may well include motivated and efficient employees. Simultaneously, human-relationship-related processes are intended for actively improving staff motivation and work satisfaction.

Training, in the upper right-hand corner of Figure 38, is an important element of the knowledge-management-based approaches to knowledge security, just as it is on the security side in Figure 37. From the knowledge management perspective, training can

refer to recognition of important knowledge, education about the work processes connected to knowledge management processes, and training in how knowledge should be recognised and valued at one's company. All of the knowledge-management-rooted approaches should be built on an organisational culture that supports according value to knowledge. This knowledge culture needs to be fostered and nurtured in order to facilitate the knowledge management processes that are in place at the company.

When the elements of threats, the characteristics of secure knowledge, and the knowledge management processes are brought together, a model can be built for the concept of knowledge security. Our model for knowledge security, which is the output of this final step of the conceptual analysis process illustrated in Figure 7 (on p. 14), is presented in Figure 39.

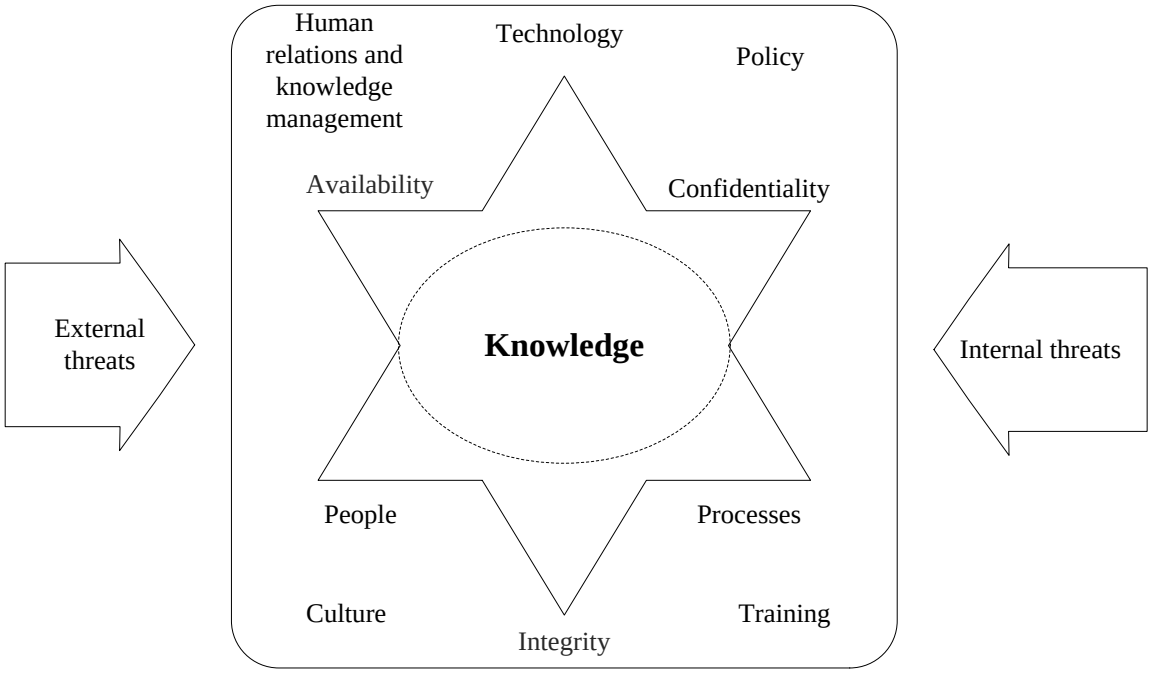

Figure 39: The knowledge security model

Diverse threats (both external and internal) need to be considered when one examines knowledge security, as is illustrated in Figure 39. The threats to a company's knowledge are more varied than just the leaking of knowledge. Employee turnover, obsolete knowledge, human mistakes, and intentional harm are all real threats and may in some cases even do more damage than a simple and small knowledge leak. The knowledge security initiatives of a company need to take these threats into account, and the more detailed CIA framework depicted in Figure 37 is one way to approach analysis of the threats.

Confidentiality is the characteristic most commonly addressed both in knowledge protection initiatives and in the information security field, and this conclusion is supported by both the theoretical and empirical findings of this study. However, the

integrity and availability of knowledge are just as important so should be adequately addressed. The various dimensions of knowledge management, illustrated in more detail in Figure 38, represent different approaches that together can be used to ensure that the knowledge has the ideal characteristics.

The final phases in the process of knowledge security illustrated in Figure 35, on page 153, are monitoring and improvement. A note made at the beginning of this section bears repeating here: the process of security is incremental, since many elements in the process are subject to constant change – the threats to knowledge change, the knowledge itself changes, and the objective of security changes. Therefore, constant monitoring of each is needed, so that they can be analysed and the activities then adjusted and improved. The managerial perspectives and tools shown in the corners of Figure 39 are one way to approach the monitoring and improvement phases of the knowledge security process.

First, illustrated in the upper right-hand corner of Figure 39, the security policies are one tool to structure the monitoring process and set requirements that can be monitored in a company. Another managerial tool shown in the figure is training. Training is a part of the improvement phase of the knowledge security process (see Figure 35, on p. 153). Training from both the knowledge management and the security perspective is beneficial for knowledge security efforts. Training employees improves their chances of recognising and addressing the threats that knowledge in the company faces. Training also affects the knowledge security culture of the company in the long run.

Although culture cannot be considered an actual managerial tool, acknowledging that the culture exists and that it can be affected is a driver for managerial decisions. The knowledge culture and security culture of a company have a great impact on how the knowledge is made and kept secure. For example, knowledge management and human relations management initiatives have an effect on company security culture. Therefore, knowledge management and human relation management initiatives can be regarded as one managerial tool that is used for security of knowledge. These management tools are aimed at the development of employee competencies and motivation, which, in turn, are related to many of the dimensions of knowledge security depicted in more detail in figures 37 and 38.

Figure 39 ties together all of the various factors found in this study that affect knowledge security in a company. That the model for the concept of knowledge security is quite complicated illustrates how very complex the concept is. However, this complexity does not mean that the concept cannot be valid. Bringing together two branches of management in one conceptual model implies that the complexities of the two fields must meet in the model. The complexity is reduced when the various aspects of the model are applied at a practical level. In practice, some aspects of the model may even seem trivial, such as documentation of employee knowledge as a way to secure

integrity and availability. The model could have numerous implications for both research and practice. These are discussed in the following section.

6.2 Discussion of implications

In this study, the conceptual analysis of the concept of knowledge security has yielded a model that describes the elements of the concept. Knowledge security is a process aimed at protection of the knowledge of the employees at a company. The knowledge security model presented in Figure 39 includes the knowledge security process, the elements of threats to knowledge, and the kinds of solutions companies can implement to address those threats. Accordingly, the framework has both theoretical and practical implications, which are discussed in subsections 6.2.1 and 6.2.2, respectively.

6.2.1 Implications for theory

The summary of the discussion on knowledge management and information security management provided at the end of Chapter 2 of this study leads to the conclusion that the two fields share approaches and challenges. By combining the perspectives of knowledge management and security, companies could gain benefit for both knowledge management and information security efforts.

The literature review presented in Section 4.1 brings insight into the two theoretical fields that form the backdrop for this study. Table 11 and Table 12 show that there is some overlap in the theory addressing a knowledge-based view and information systems, but overlap in the existing literature between information security management and knowledge management is minimal. One motivation for this study was to show that extending the overlap could yield benefits for both fields. This motivation is illustrated in Figure 40.

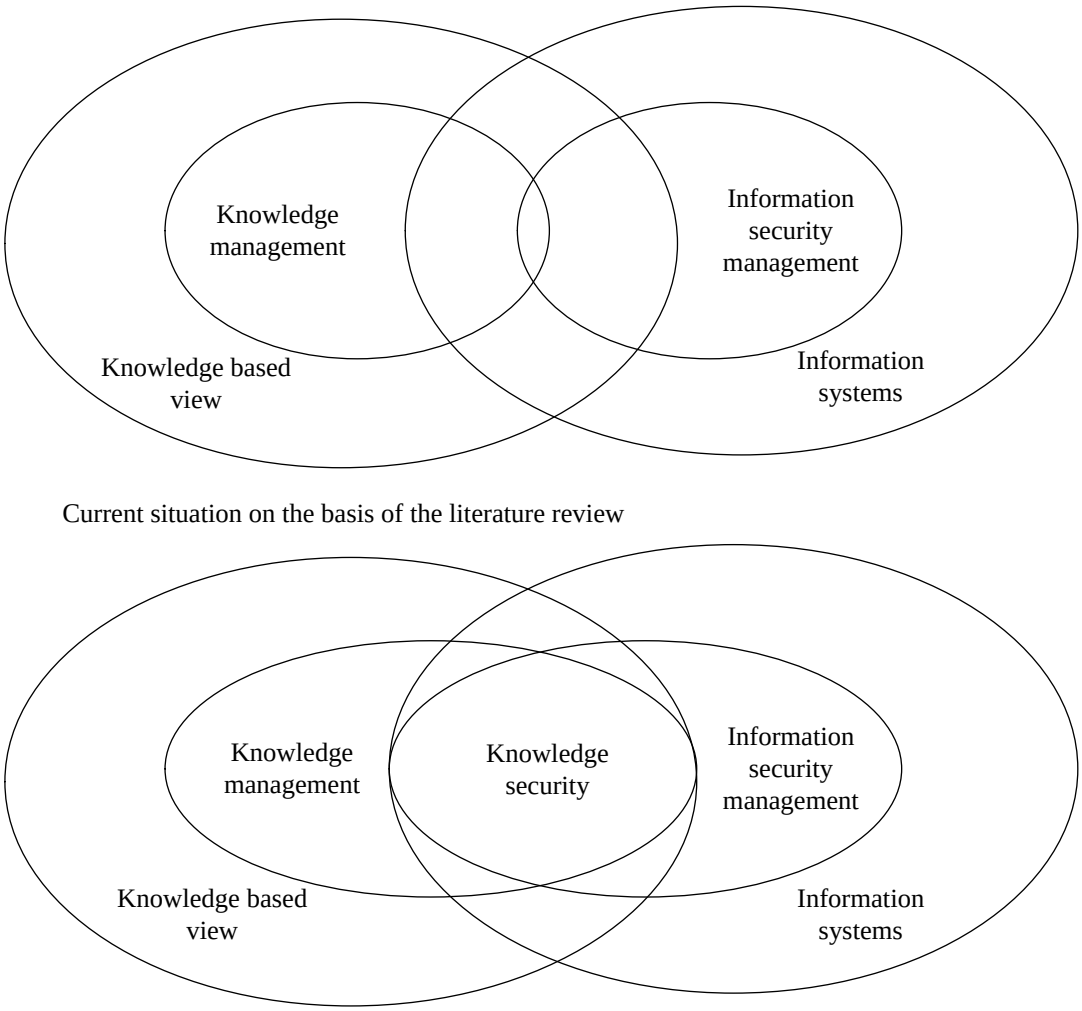

Figure 40: The overlap of the fields of theory

In Figure 40, a picture of the existing situation emerging from the literature review presented in this study is provided in the upper illustration. It shows very little overlap between the fields of knowledge management and information security management. The potential in wider acceptance of the knowledge security concept is shown in the figure's lower pane. Conscious combination of the security management and knowledge management perspectives to knowledge would bring information security management and knowledge management into greater overlap and bring forth mutual benefits.

A valid theoretical contribution extends existing theory to a new setting and at the same time adds something to it (Whetten 1989). In this study, the information security management frameworks of a security management process and the characteristics for secure information have been applied to the concept of knowledge security. Clearly, these seemingly separate fields of theory can bring valuable contributions to each other.

The overlap of theoretical fields that is found in this study can be illustrated in terms of perspectives that the individual theoretical fields or concepts contribute to each other.

The concept of knowledge security interfaces with parallel concepts and areas of theory that can reap new perspectives and ideas as fruit of this study. These contributions are examined in Figure 41. The parallel concepts and theoretical fields are not entirely comparable with each other, although they are illustrated as if they were. The purpose of Figure 41 is to illustrate the interfaces of the concept of knowledge security, not so much to represent the positions of the parallel concepts in relation to each other.

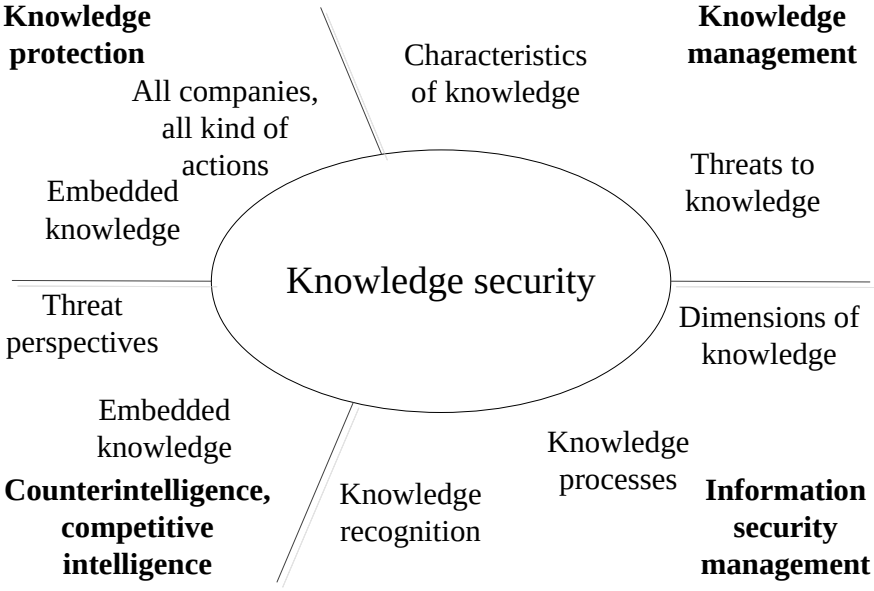

Figure 41: Links of knowledge security to parallel concepts

The synthesis from the two theoretical fields brings the perspective of security to the field of knowledge management and carries the understanding of the dimensions of knowledge to the field of information security. Each field brings valuable contributions to the other, and the strength of the knowledge security concept comes from the strengths of both informing background fields. The contribution of the knowledge management field to the concept of knowledge itself is the perspective of recognition and management processes. Knowledge management processes can aid with security of knowledge that otherwise would fall outside the scope of information security activities. Meanwhile, the contribution of the information security field to knowledge management is the perspective of several characteristics that need to be ensured via a company's management initiatives. Another contribution to the field of knowledge management is the perspective of threats. Knowledge security begins with the recognition of important knowledge, followed by recognition of the threats that the knowledge faces.

The concept of knowledge protection is very close to that of knowledge security, but the scope of the former is much narrower. The concept of knowledge security brings a wider perspective of examining all activities of a company from the angle of security and protection, rather than concentrating merely on the context of collaboration and alliances between companies. In the context of alliances, the concept of knowledge security can

be considered very close to knowledge protection. However, knowledge security work examines also threats that exist in companies regardless of any collaboration, of whatever type, with other companies. Knowledge protection as a concept also concentrates a great deal on knowledge that has an explicit form and, accordingly, can be protected by legal means. In this sense, the two concepts are complementary, since knowledge security concentrates on knowledge that is embedded in people and, hence, mostly in tacit form.

The interface between the concept of knowledge security and that of counterintelligence or competitive intelligence is found in the perspective of threats. The intelligence functions in a company can contribute to the knowledge security process by discussing their goals. A company's intelligence goals can often reveal threats that competitors may cause to the company's knowledge, since what one company wants to know about its competitors is most likely the same type of thing those competitors want to know about said company. The perspective of knowledge security on the counterintelligence efforts of a company is that there is a lot of knowledge embedded in people and that intelligence should target that knowledge, both from the standpoint of protecting what the company has and from the angle of gaining knowledge from competitors.

From the research point of view, a clear implication for theory emerges from the systematic review presented in this study. The concept of knowledge security is new, and it has not been systematically studied before, though the review showed that some authors do use the concept. The parallel concepts analysed in this study are very close to the concept of knowledge security, but they are focused on narrow areas such as competitive intelligence or strategic alliances of companies. However, knowledge needs to be secure in all aspects of the operations of a company, and drawing together these narrower concepts under the umbrella of knowledge security could aid in locating areas wherein the security perspective on knowledge has not yet been considered. When knowledge security is combined with the wide perspectives of information security and knowledge management, companies can develop a well-functioning entity of data, information, and knowledge that is both used efficiently in the company and secured reasonably, so that the operations of the company are not threatened.

6.2.2 Implications for practice

This study is highly theoretical in nature, as conceptual research tends to be. The core result of the study is a definition and model for a theoretical concept. Regardless of its theoretical orientation, the conceptual analysis has empirical elements and, through these, can have practical implications too. After all, a concept brings together a term, a definition, and a phenomenon (Niiniluoto 1984). The practical contribution of this study is the recognition of a phenomenon called knowledge security. The phenomenon should be further studied in practice, in application of the model developed in this study to companies' operations and analysis of its contributions through explicit measurements.

Companies can find interesting insights from the empirical analysis. While the companies in the empirical study did not employ the concept of knowledge security, they all worked for secure knowledge in some way. By systematising their approach to knowledge and combining the perspectives of knowledge management and information security, they might improve their results in both areas. The protection mechanisms identified from the interview materials were not all consciously recognised as knowledge protection mechanisms by the participating companies. By bringing the knowledge security process framework into use, the companies could go to conscious effort to make their knowledge secure. They should recognise their important knowledge, identify the threats it faces, and analyse the protection mechanisms that they already have in place. On the basis of the current situation, companies can plan improvements in their protection mechanisms. The model presented in Figure 39 (see p. 158) can be applied by any company wishing to address knowledge security in its activities.

The impact of the concept of knowledge security on the operations of companies need not be big. The changes in perspective in individual processes may be very small, but they could add up to substantial changes in the security status of the company. Adding the perspective of risks and threats to knowledge management initiatives may help to uncover areas in which knowledge is not, in fact, managed, and where it should be protected better. When the knowledge security process is embedded in everyday management, considering the perspective of threats to knowledge should be as automatic as thinking from the perspective of what knowledge is needed for operations.

A knowledge-based perspective on information security training could help the companies as they contemplate what kind of training they should offer to their employees and consider its topics. The findings from the interviews suggest that managers may well recognise important knowledge differently from their subordinates. Knowledge security training can offer a way to bridge the gap and come to better understanding of what the important knowledge is. Traditional information security training is not very interactive. Instead, it is conducted with a format that involves providing many receivers with information about the approved work practices and the ways in which one is required to use the information systems. This kind of training does not take into account the various ways in which recipients might interpret the meaning of information security, let alone knowledge security. Differing understandings of what is valuable and how it should be protected can be harmful to protection initiatives.

In contrast, knowledge security training could challenge the employees to recognise which knowledge is important from their point of view and then identify threats to that knowledge. Instead of one person lecturing, the whole group of personnel could participate in first specifying what the company actually needs to protect and the kinds of threats against which it is to be protected. The characteristic-based approach to knowledge discussed in this study could be utilised in such training sessions.

The cultural aspects of knowledge security are another area of practical contribution. The combination of various cultural perspectives on knowledge and security can help companies to recognise the dual effect of culture on knowledge security: it is both a threat and a protection mechanism, and neither of these aspects should be neglected. Harnessing the culture is challenging for many companies but is important. The vital role of the culture is emphasised in the empirical results of this study.

In summary of the practical implications of knowledge security, one can state that the concept provides a model for managers' use to address threats to knowledge in a company and that, thereby, it complement both information security activities and knowledge management activities that might already be performed at their company. The knowledge security model can, of course, be utilised even in the absence of systematic knowledge management at the company, in which case it could serve as a way to begin development of knowledge management. The knowledge security model provides a management tool for recognising important knowledge and starting to address the threats that knowledge faces. Many information security risks are considered to be caused by people (e.g., von Solms & von Solms 2004a, Peltier et al. 2005). Therefore, the concept of knowledge security provides a good way to get a better perspective on the human side of information security.

6.3 Evaluation of the study

This research has utilised qualitative methods. The criteria for evaluating the results of qualitative research involve evaluation of the results as having validity, reliability, and generalisability (Guba & Lincoln 1985, Yin 1994, Gummesson 2006, Saunders et al. 2009) or, in other terms, evaluation of the credibility, transferability, dependability, and confirmability of the research (Guba & Lincoln 1985). Although the latter set of evaluation criteria is specific to qualitative research, a strong argument has been made for using the same terms in evaluation of both quantitative and qualitative research (Morse et al. 2008). Accordingly, the widely used research evaluation criteria of reliability, validity, and generalisability are chosen as criteria for evaluation of this study. In the following sections, these elements are discussed in turn. At the end of this section, directions for further studies in this field are discussed.

6.3.1 Validity

Validity of research refers to whether the research studies the phenomenon it claims to study (Saunders et al. 2009). In other words, the validity of research can be evaluated through examination of how well it answers the research questions that it set for itself. The introduction to this study presented the research questions and research approach. The primary research question for this study was

What is knowledge security?

The approach chosen for answering this research question was conceptual analysis. The question was further divided into two sub-questions:

a) How are knowledge security and related concepts defined and referred to in contemporary literature?

The systematic literature review in Chapter 4 answers this question by peering into where the concept of knowledge security is used and with what meaning it is used. One incidental finding from the review is that the top journals in the background theoretical fields are not the arena for discussion of knowledge security. A reason for this may be found in the concept's position between theoretical fields: the top journals are not always keen to publish research that is not in the core focus of their research field. Another reason for this situation may be that knowledge security as a research topic is still young and is not mature enough to be addressed in high-standard publication fora.

Before the systematic literature review, the background theoretical fields informing this study were subjected to theoretical examination. The fields' differences in approach and their common elements were discussed. The analysis of the theoretical fields shows that the concept of knowledge security fits very well between the fields and that it can be used as a way of lowering barriers between the fields.

Triangulation increases the validity of research (Denzin 1978). In the case of research question **a**, triangulation was achieved through data triangulation. The literature analysed in the review was collected from a range of journals and from many databases, for capture of as many relevant articles as possible.

b) How do companies secure knowledge?

The introductory empirical study showed that the approach of knowledge security could be very relevant for companies. The results from the introductory material provide further motivation for analysis of the concept. This study also reveals a challenge related to attitudes: if companies consider security of knowledge impossible, is it thus rendered impossible? The introductory study reveals interesting attitudes toward information security and potentially knowledge security at the participating companies, but the introductory study does not actually answer research question **b**.

The primary empirical study was conducted to find out whether the phenomenon of knowledge security exists and how companies approach making knowledge secure. The results of the primary study show that, although the companies did not use the term 'knowledge security', the phenomenon is recognised. The personnel being interviewed indicated that the topic was challenging for them to discuss, and they acknowledged that the security of knowledge cannot be the responsibility of just one person. The term

‘knowledge security’ describes a multifaceted phenomenon that has to do with knowledge in many forms and locations.

For question **b** too, triangulation was achieved through data triangulation (Denzin 1978), since the research method used was the same, interviews and content analysis, in the two studies. Some method triangulation was achieved through the presence of students in the introductory study. This brought many interviewers – and consequently more questions – to the interviews. However, the role of this triangulation from the standpoint of the present study is not very large, since the role of the introductory study is not so great.

When the two sub-questions for the research were answered, their answers could be combined to form an answer to the primary research question, and our definition for knowledge security was presented in Section 6.1. The research findings suggest that the concept of knowledge security exists and that it can be defined through application of theoretical analogies from the information security and knowledge management fields. The definition also draws from parallel concepts and empirical findings related both to threats facing knowledge and to protection mechanisms.

This study has followed the conceptual analysis approach to research. The aim of the conceptual analysis process is to gain an understanding of the concept and finally present its implications for the theoretical context. All of the steps of conceptual analysis that were described in the introduction have been followed in this study, and a definition of the concept was presented alongside theoretical and practical implications.

6.3.2 Reliability

In the previous section, the validity of research is described as the degree to which the study addresses the phenomenon that it is supposed to study. Reliability of research refers to how much the results of the research depend on the researcher and on the particular data gathered for the research. In other words, how reliable the research is depends on whether the same results would be reached if someone else were to repeat the research process or analyse the same data (Yin 1994, Gummesson 2006). According to Easterby-Smith et al. (2008), the following questions can be utilised when one is assessing reliability:

- Is it possible to see the route from the data to the conclusions?
- Could another researcher come to the same conclusions?
- Would the same results be achieved if the work were repeated on another occasion?

Let us consider the first of these questions first. The data collection methods used in this research are thoroughly described in sections 3.1 and 5.1, along with the analysis methods utilised in the study. Also, the literature review has been reported upon in a

transparent way, to show the origins of the theoretical data. Thorough description of data collection and analysis is one way to show the route from the data to the conclusions (Douglas 1971, Easterby-Smith et al. 2008). Therefore, the study meets the first criterion for reliable research.

The second question stated by Easterby-Smith et al. (2008) considers the dependence of the results on the researcher. The role of the researcher is large in hermeneutic research, and the results depend on interpretations by the person carrying out the analysis (Metsämuuronen 2005). Each person interprets interviews differently, and the interpretation depends heavily on the background of the researcher. Someone with a background in other fields may have paid attention to entirely different issues in the interview material. From this angle, the reliability of the research could be questioned. However, this reliability challenge is accepted as a characteristic of qualitative research (Yin 1994, Mansourian 2008). Bigger research projects often address this weakness by having more than one person analyse the qualitative data (Yin 1994, Metsämuuronen 2005). Increasing the number of people conducting the analysis reduces dependence on the interpretation of just one person. In the case of the present work, however, this was not possible. The weakness has been addressed instead through the use of interview extracts to illustrate the kinds of material the interview data include and how the researcher has interpreted them.

The last question presented by Easterby-Smith et al. (2008) considers the repeatability of the study, along with dependence on time. The concept of knowledge security is a construct of information security- and knowledge management-based approaches to knowledge embedded in people. The interview results might be different if the study were to be repeated in the future. This is because the understanding of knowledge changes, as do the threats to knowledge. However, the dynamics of the concept are not thought to change rapidly, and the results would be quite similar if the study were repeated soon.

Another approach to reliability is to consider the degree to which the interviews give an accurate description of the situation of the participating companies. However, since the aim of this study was to gain a preliminary understanding of the concept of knowledge security, to what extent the answers of the interviewees represent the companies they represented is not as important as it would be if the companies were being compared with each other. The interviews considered matters from the full-company perspective, but the researcher has borne in mind that some of the answers may represent personal opinions rather than the company-wide approach. One reason for such disparity may be that knowledge security was not addressed at the companies through conscious effort and, therefore, company-wide understanding of the notion and application did not exist.

6.3.3 Generalisability

Generalisability, or external validity, of qualitative research is a dimension that does not always receive much attention in evaluation (Schofield 2002). Some authors claim that generalisability of qualitative research results should not be the goal in the first place and, accordingly, that generalisability need not be evaluated (Myers 2000). However, dismissing its evaluation by pointing out that it was not sought is not the option chosen for this study. There are elements of generalisability in this work, although they need to be discussed in terms of generalisability from a qualitative rather than quantitative perspective.

Schofield (2002) describes generalisability of qualitative research as able to be linked to the perspectives of *what is*, *what may be*, and *what could be*. These targets influence the selection of data sources, in view of reaching the target. If a good picture of *what is* is the core aim, the data should be collected from typical environments so that they can be assumed to represent other typical contexts well. A target involving *what is* requires also multiple sites of enquiry. If the target is to explore *what may be*, the research should be focused on finding contexts that are ahead of their time and represent phenomena that could become more commonplace with the passing of time. When the target is to find out *what could be*, the goal of the research is to find settings that are found to represent ideal qualities. In this case, the focus is on uncovering what is going on in an environment that is by some criteria considered to represent the ideal (Schofield 2002).

When one examines this study from the perspective of the possible targets presented by Schofield (2002), it is clear that the main target of the empirical studies for this work has been to find out *what is* the information security status of companies (in the introductory study) and *what is* knowledge security at companies (in the primary study). Whether the companies that participated in these studies represent typical cases can, however, be questioned. The companies that took part in the studies were not selected on the basis of any specific criteria through which they would stand out from any other companies. In this sense, they can be considered typical examples.

Although the term ‘sampling’ is used mainly in quantitative research and is an essential element in judging the generalisability of quantitative research, the word is employed also in connection with qualitative research (Marshall 1996). The sampling method used in this study is mainly judgement sampling – with, more specifically, a maximum variation sample in the primary study. The companies that were involved in the study represent different industries and different sizes of organisation, so they vary greatly in their operations. Common to all of the companies is heavy reliance on knowledge, and they all engaged in international operations in that they had operations in more than one country and were serving an international market. In this sense, the companies have both common and widely varying characteristics so provide quite a broad picture of what knowledge security means for companies.

An element of convenience sampling is always present in qualitative research, because only companies that are accessible to the researcher end up being in the sample. This element is stronger in the introductory study, since the companies had to be selected on the basis of location and access. If sampling could have been done only by judgement sample, larger and more varied companies would have participated. The problem of access, however, is common in all research; it is no bigger an issue in this study.

Although the results presented in this study cannot be claimed to be statistically representative of a population of companies, a tentative generalisation can be, and is, offered in the final results of the study. The elements of threats to knowledge and knowledge protection mechanisms that were identified from the interviews at the companies can be tentatively generalised to an approach to knowledge at all companies. Similar discussions from very different companies show that there are some general elements of knowledge security that are not dependent on company size, location, or industry. Of course, all of the companies that took part in the research have their headquarters in Finland, which limits the generalisation to the level of Finland or perhaps small Western countries. Further studies could extend the exploration of the knowledge security phenomenon to other countries and cultures.

6.3.4 Future points of interest

This study suggests an acknowledgement of overlap between the knowledge management and information security fields. Future studies could take the conjunction of the security and knowledge management fields under broader examination. The perspective of security could be incorporated into many knowledge management studies. The perspective of knowledge that is embedded in people could be added to information security studies, to widen the range of threats on which the studies focus. The challenge in this theoretical research is the elusiveness of the concept of knowledge. It may be difficult to measure and quantify, while concentrating on information that is more easily tackled is much simpler. However, knowledge is recognised as an important asset to companies, so it should be given attention in research too. Application of experience in ways of measuring the value of intellectual capital could be useful for the field of knowledge security.

Further studies of this topic could evaluate the usefulness of the knowledge security model in structuring of training to be offered to employees. Information security training has received quite a lot of attention from the perspective of appropriate work habits and of how the training affects the information security culture (Whitman & Mattord 2003, Thomson et al. 2006, D'Arcy et al. 2009, Myyry et al. 2009). The combination of recognising important knowledge and then analysing the threats that knowledge faces could prove to be an efficient way of promoting awareness of both knowledge security and knowledge management in a broader sense. Therefore, this

training-oriented avenue for future research seems a very interesting space wherein the approaches of knowledge management and information security could be combined.

Knowledge management research has addressed knowledge protection through quantitative studies. Those studies have identified some threats to knowledge, yet the results of the present study indicate that the perspectives taken to threats to knowledge are narrow. In view of this, future quantitative studies could broaden the perspective on knowledge protection as one element of knowledge management, and address other threats to knowledge than merely knowledge leaks. In a sense, other threats are tackled by way of knowledge management elements such as knowledge codification and the sharing and transfer of knowledge. However, researchers need both to recognise that these are applied to counter threats to knowledge and at the same time to acknowledge that the same activities may actually cause threats if not managed properly.

In the introductory chapter of this work, strategic management was excluded from the scope of study. However, the close connection of the emergence of security practices to the emergence of a company's strategy practices certainly could be researched, and the focus of attention shifted to, for example, individual workers as champions of security practices and their impact on the organisation's security culture. This line of research could explore the practical dimension of the concept of knowledge security and also contribute to the information security field in general.

Bibliography

Alavi, M. & Leidner, D.E. 2001. "Review: Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues". MIS Quarterly. vol. 25, no. 1. pp. 107-136.

Albrechtsen, E. 2007. "A qualitative study on users' view on information security". Computers & Security. vol. 26. pp. 276-289.

Anderson, C.L. & Agarwal, R. 2010. "Practicing Safe Computing: a Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions". MIS Quarterly. vol. 34, no. 3. pp. 613-643.

Argote, L. & Ingram, P. 2000. "Knowledge Transfer: A Basis for Competitive Advantage in Firms". Organizational behavior and human decision processes. vol. 82, no. 1. pp. 150-169.

Argote, L., McEvily, B. & Reagans, R. 2003. "Managing Knowledge in Organizations: An Integrative Framework and Review of Emerging Themes". Management Science. vol. 49, no. 4, Special Issue on Managing Knowledge in Organizations: Creating, Retaining, and Transferring Knowledge. pp. 571-582.

Assudani, R.H. 2009. "Dispersed knowledge work – implications for knowledge intensive firms". Journal of Knowledge Management. vol. 13, no. 6. pp. 521-532.

Awad, E. & Ghaziri, H. 2004. Knowledge Management. Prentice Hall, Upper Saddle River, New Jersey.

Baloh, P., Jha, S. & Awazu, Y. 2008. "Building strategic partnerships for managing innovation outsourcing". Strategic Outsourcing: An International Journal. vol. 1, no. 2. pp. 100-121.

Barachini, F. 2009. "Cultural and social issues for knowledge sharing". Journal of Knowledge Management. vol. 13, no. 1. pp. 98-110.

Barman, S. 2001. Writing Information Security Policies. New Riders, Indianapolis.

Barney, J. 1991. "Firm Resources and Sustained Competitive Advantage". Journal of Management. vol. 17, no. 1. pp. 99-120.

Baskerville, R. F. 2003. "Hofstede never studied culture". Accounting, Organizations and Society, vol. 28, no. 1. pp. 1–14

Baughn, C.C., Denekamp, J.G., Stevens, J.H. & Osborn, R.N. 1997. "Protecting intellectual capital in international alliances". Journal of World Business. vol. 32, no. 2. pp. 103-117.

Baxter, R. & Matear, S. 2004. "Measuring intangible value in business-to-business buyer–seller relationships: An intellectual capital perspective". Industrial Marketing Management. vol. 33, no. 6. pp. 491-500.

Belsis, P., Kokolakis, S. & Kiountouzis, E. 2005. "Information systems security from a knowledge management perspective". Information Management & Computer Security. vol. 13, no. 3. pp. 189-202.

Blackler, F. 1995. "Knowledge, Knowledge Work and Organizations: An Overview and Interpretation". Organization Studies. vol. 16, no. 6. pp. 1021-1046.

Bock, G.W. & Kim, Y.G. 2002. "Breaking the myths of rewards: an exploratory study of attitudes about knowledge sharing". Information Resources Management Journal. vol. 15, no. 2. pp. 14-21.

Boella, G. & van der Torre, L. 2006. "Security Policies for Sharing Knowledge in Virtual Communities". IEEE Transactions on systems, man, and cybernetics – Part A: Systems and Humans. vol. 36, no. 3. pp. 439-450.

Bojanc, R. & Jerman-Blažič, B. 2008. "An economic modelling approach to information security risk management". International Journal of Information Management. vol. 28, no. 5. pp. 413-422.

Bontis, N. 1998. "Intellectual capital: an exploratory study that develops measures and models". Management Decision. vol. 36, no. 2. pp. 63-76.

Bontis, N. & Serenko, A. 2009. "A follow-up ranking of academic journals". Journal of Knowledge Management. vol. 13, no. 1. pp. 16-26.

Bose, R. 2003. "Knowledge management-enabled health care management systems: capabilities, infrastructure, and decision-support". Expert Systems with Applications. vol. 24, no. 1. pp. 59-71.

Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. & Boss, R.W. 2009. "If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security". European Journal of Information Systems. vol. 18, no. 2 Special Issue: Behavioral and Policy Issues in Information. pp. 151-164.

Brockmann, E.N. & Anthony, W.P. 2002. "Tacit Knowledge and Strategic Decision Making". Group & Organization Management. vol. 27, no. 4. pp. 436-455.

Brunold, J. & Durst, S. 2012. "Intellectual capital risks and job rotation". Journal of Intellectual Capital. vol. 13, no. 2. pp. 178-195.

Bueno, E., Salmador, M. P., & Rodríguez, Ó.. "The role of social capital in today's economy: Empirical evidence and proposal of a new model of intellectual capital". Journal of Intellectual Capital. vol. 5, no. 4. pp. 556-574.

Bulcuru, B., Cavusoglu, H. & Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness". MIS Quarterly. vol. 34, no. 3. pp. 523-548.

Burrell, G. & Morgan, G. 1979. Sociological paradigms and organisational analysis. Ashgate publishing company, Burlington.

Chai, K. & Nebus, J. 2012. "Personalization of Codification? A Marketing Perspective to Optimize Knowledge Reuse Efficiency". IEEE Transactions on Engineering Management. vol. 59, no. 1. pp. 33-51.

Chauvel, D. & Despres, C. 2002. "A review of survey research in knowledge management: 1997-2001". Journal of Knowledge Management. vol. 6, no. 3. pp. 207-223.

Chen, T. 2008. "Knowledge sharing in virtual enterprises via an ontology-based access control approach". Computers in Industry. vol. 59, no. 5. pp. 502-519.

Chi, L. & Holsapple, C.W. 2005. "Understanding computer-mediated interorganizational collaboration: a model and framework". Journal of Knowledge Management. vol. 9, no. 1. pp. 53-75.

Chiravuri, A., Nazareth, D. & Ramamurthy, K. 2011. "Cognitive Conflict and Consensus Generation in Virtual Teams During Knowledge Capture: Comparative Effectiveness of Techniques". Journal of Management Information Systems. vol. 28, no. 1. pp. 311-350.

Choi, B. & Lee, H. 2002. "Knowledge management strategy and its link to knowledge creation process". Expert Systems with Applications. vol. 23, no. 2. pp. 173-187.

Choo, C.W. 2002. Information Management for the Intelligent Organization. The Art of Scanning the Environment. 3rd edition ed. Information Today, Medford.

Choo, C.W. 1996. "The knowing organization: How organizations use information to construct meaning, create knowledge and make decisions". International Journal of Information Management. vol. 16, no. 5. pp. 329-340.

Chou, P.B. & Passerini, K. 2009. "Intellectual property rights and knowledge sharing across countries". Journal of Knowledge Management. vol. 13, no. 5. pp. 331-344.

Chua, A. 2009. "The dark side of successful knowledge management initiatives". Journal of Knowledge Management. vol. 13, no. 4. pp. 32-40.

Chua, A. & Lam, W. 2005. "Why KM projects fail: a multi-case analysis". Journal of Knowledge Management. vol. 9, no. 3. pp. 6-17.

Clarke, N.L. & Furnell, S.M. 2007. "Advanced user authentication for mobile devices". Computers & Security. vol. 26, no. 2. pp. 109-119.

Clarke, S. 2000. "Safety culture: under-specified and overrated?". International Journal of Management Reviews. vol. 2, no. 1. pp. 65-90.

Collins English Dictionary. 2006. 8th ed. Harper Collins Publishers.

Collins, R.J. 1997. Better Business Intelligence. How to Learn More About Your Competitors. Management Books 2000, Chalford.

Cooper, M.D. 2000. "Towards a model of safety culture". Safety Science. vol. 36, no. 2. pp. 111-136.

Crossler, R. & Bélanger, F. 2009. "The Effects of Security Education Training and Awareness Programs and Individual Characteristics on End User Security Tool Usage". Journal of Information System Security. vol. 5, no. 3. pp. 3-22.

Czejdo, B.D. & Morzy, T. 2008. "Knowledge, Knowledge Security, and Meta-knowledge". Open Knowledge Society: a Computer Science and Information Systems Manifesto. vol. 19, pp. 245-252.

D'Arcy, J., Hovav, A. & Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach". Information Systems Research. vol. 20, no. 1. pp. 79-98.

Daintith, J. & Wright, W. 2012. A Dictionary of Computing. Online ed. Oxford University Press.

Davenport, T. & Prusak, L. 1998. Working Knowledge. How organizations manage what they know. Harvard Business School Press.

Davenport, T.H., De Long, D.W. & Beers, M.C. 1998. "Successful knowledge management projects". Sloan management review. vol. 39, no. 2. pp. 43-57.

Davis, J.J. & Clark, A.J. 2011. "Data preprocessing for anomaly based network intrusion detection: A review". Computers & Security. vol. 30, no. 6. pp. 353-375.

de Faria, P. & Sofka, W. 2010. "Knowledge protection strategies of multinational firms - A cross-country comparison". Research Policy. vol. 39, pp. 956-968.

De Long, D.W. 2004. Lost Knowledge - confronting the threat of an aging workforce. Oxford University Press, New York.

De Long, D. & Fahey, L. 2000. "Diagnosing Cultural Barriers to Knowledge Management". The Academy of Management Executive. vol. 14, no. 4.

Dean, J.W.,Jr. & Sharfman, M.P. 1996. "Does Decision Process Matter? A Study of Strategic Decision-Making Effectiveness". The Academy of Management Journal. vol. 39, no. 2. pp. 368-396.

Denison, D.R. 1996. "What is the Difference between Organizational Culture and Organizational Climate? A Native's Point of View on a Decade of Paradigm Wars". The Academy of Management Review. vol. 21, no. 3. pp. pp. 619-654.

Denison, D.R., Haaland, S. & Goelzer, P. 2003, "Corporate culture and organizational effectiveness: is there a similar pattern around the world?" in Advances in Global Leadership, Volume 3 Emerald Publishing Limited, , pp. 205-227.

Denzin, N.K. 1978. The Research Act. 2nd ed.McGraw-Hill, New York.

Desouza, K.C. 2007. Knowledge Security: Protecting your company's intellectual assets.

Desouza, K.C. 2006. "Knowledge Security: An Interesting Research Space". Journal of Information Science & Technology. vol. 3, no. 1. pp. 1-7.

Desouza, K.C. & Vanapalli, G.K. 2005. "Securing knowledge in organizations: lessons from the defense and intelligence sectors". International Journal of Information Management. vol. 25, no. 1. pp. 85-98.

Devadason, F.J. & Lingam, P.P. 1997. "A methodology for the identification of information needs of users". IFLA Journal. vol. 23, no. 1. pp. 41-51.

Díaz-Cabrera, D., Hernández-Fernaud, E. & Isla-Díaz, R. 2007. "An evaluation of a new instrument to measure organisational safety culture values and practices". Accident Analysis & Prevention. vol. 39, no. 6. pp. 1202-1211.

Ding, X., Liu, H. & Song, Y. 2013. "Are internal knowledge transfer strategies double-edged swords?". Journal of Knowledge Management. vol. 17, no. 1. pp. 69-86.

Donate, M.J. & Canales, J.I. 2012. "A new approach to the concept of knowledge strategy". Journal of Knowledge Management. vol. 16, no. 1. pp. 22-44.

Douglas, J.D. 1971. Understanding Everyday Life: Toward the Reconstruction of Sociological Knowledge. Routledge & Kegan Paul, London.

Drott, M. 2001. "Personal Knowledge, Corporate Information: The Challenges for Competitive Intelligence". Business Horizons. vol. 44, no. 2. pp. 31-37.

Durcikova, A., Fadel, K.J., Butler, B.S. & Galletta, D.F. 2011. "Knowledge Exploration and Exploitation: The Impacts of Psychological Climate and Knowledge Management System Access". Information Systems Research. vol. 22, no. 4. pp. 855-866.

Dutta, A. & McCrohan, K. 2002. "Management's Role in Information Security in a Cyber Economy". California management review. vol. 45, no. 1. pp. 67-87.

Easterby-Smith, M., Thorpe, R., Jackson, P. & Lowe, A. 2008. Management Research. 3rd ed. Sage, London.

Elo, S. & Kyngäs, H. 2008. "The qualitative content analysis process". Journal of Advanced Nursing. vol. 62, no. 1. pp. 107-115.

Endres, M.L., Endres, S.P., Chowdhury, S.K. & Alam, I. 2007. "Tacit knowledge sharing, self-efficacy theory, and application to the Open Source community". Journal of Knowledge Management. vol. 11, no. 3. pp. 92-103.

Ergazakis, K., Metaxiotis, K., Psarras, J. & Askounis, D. 2006. "A unified methodological approach for the development of knowledge cities". Journal of Knowledge Management. vol. 10, no. 5. pp. 65-78.

Fontana, A. & Frey, J. 2005, "The Interview – From Neutral Stance to Political Involvement." in The SAGE Handbook of Qualitative Research., eds. N.K. Denzin & Y. Lincoln, 3rd ed, SAGE, London, pp. 695-727.

Ford, D.P. & Staples, S. 2010. "Are full and partial knowledge sharing the same?". Journal of Knowledge Management. vol. 14, no. 3. pp. 394-409.

Frishammar, J. 2003. "Information Use in Strategic Decision Making". Management Decision. vol. 41, no. 4. pp. 318-326.

Fuchs, L., Pernul, G. & Sandhu, R. 2011. "Roles in information security – A survey and classification of the research area". Computers & Security. vol. 30, no. 8. pp. 748-769.

Fuld, L.M. 1991. "A Recipe for Business Intelligence Success". The Journal of Business Strategy. vol. 12, no. 1. pp. 12-17.

Fung, W.S.L. & Fung, R.Y.K. 2008, "Knowledge Security for Hospitality Industry", In Marketing and management sciences, eds. D.P. Sakas & N. Konstantopoulos, Imperial college press, Covent Garden, pp. 308.

Furnell, S.M., Bryant, P. & Phippen, A.D. 2007. "Assessing the security perceptions of personal Internet users". Computers & Security. vol. 26, no. 5. pp. 410-417.

Furnell, S., Tsaganidi, V. & Phippen, A. 2008. "Security beliefs and barriers for novice Internet users". Computers & Security. vol. 27, no. 7. pp. 235-240.

Gerber, M. & von Solms, R. 2001. "From Risk Analysis to Security Requirements". Computers & Security. vol. 20, no. 7. pp. 577-584.

Gold, A.H., Malhotra, A. & Segars, A. 2001. "Knowledge Management: An Organizational Capabilities Perspective". Journal of Management Information Systems. vol. 18, no. 1. pp. 185-214.

Grant, R.M. 1996. "Toward a Knowledge-Based Theory of the Firm". Strategic Management Journal. vol. 17, Special Issue: Knowledge and the Firm. pp. 109-122.

Grote, G. 2007. "Understanding and assessing safety culture through the lens of organizational management of uncertainty". Safety Science. vol. 45, no. 6. pp. 637-652.

Guba, E.G. & Lincoln, Y.S. 1985. Naturalistic inquiry. Vol. 75 ed. Sage, California.

Guldenmund, F.W. 2000. "The nature of safety culture: a review of theory and research". Safety Science. vol. 34, no. 1-3. pp. 215-257.

Gummesson, E. 2006. "Qualitative Research in Management: Addressing Complexity, Context and Persona". Management Decision. vol. 44, no. 2. pp. 167-179.

Guo, K.H., Yuan, Y., Archer, N.P. & Connelly, C.E. 2011. "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model". Journal of Management Information Systems. vol. 28, no. 2. pp. 203-236.

Guthrie, J., Petty, R., Yongvanich, K. & Ricceri, F. 2004. "Using content analysis as a research method to inquire into intellectual capital reporting". Journal of Intellectual Capital. vol. 5, no. 2. pp. 282-293.

Hansen, M.T., Nohria, N. & Tierney, T. 1999. "What's Your Strategy for Managing Knowledge?". Harvard Business Review. vol. 77, no. 3-4. pp. 106-116.

Hansen, M.T. 1999. "The Search-Transfer Problem: The Role of Weak Ties in Sharing Knowledge across Organization Subunits". Administrative Science Quarterly. vol. 44, no. 1.pp. 82-111.

Harvey, J., Bolam, H., Gregory, D. & Erdos, G. 2001. "The effectiveness of training to change safety culture and attitudes within a highly regulated environment". Personnel Review. vol. 30, no. 6. pp. 615-636.

Hedin, H., Hirvensalo, I. & Vaarnas, M. 2011. The Handbook of Market Intelligence - Understand, Compete and Grow in Global Markets. John Wiley & Sons Ltd., West Sussex.

Helms, M., Ettkin, L. & Morris, D. 2000. "Shielding your company against information compromise". Information Management & Computer Security. vol. 8, no. 3. pp. 117-130.

Herath, T. & Rao, H.R. 2009. "Protection motivation and deterrence: a framework for security policy compliance in organisations". European Journal of Information Systems. vol. 18, no. 2 Special Issue: Behavioral and Policy Issues in Information. pp. 106-125.

Herring, J.P. 1999. "Key Intelligence Topics: A Process to Identify and Define Intelligence Needs". Competitive Intelligence Review. vol. 10, no. 2. pp. 4-14.

Hislop, D. 2005. Knowledge Management in Organizations - a critical introduction. Oxford University Press, New York.

Hofstede, G. H. 2001. Culture's consequences: Comparing values, behaviours, institutions and organizations across nations. Sage, Thousand Oaks.

Hofstede, G. H. 2003. ”What is culture? A reply to Baskerville”. Accounting, Organizations and Society. vol. 28, no. 7-8. pp. 811-813.

Holste, J.S. & Fields, D. 2010. "Trust and tacit knowledge sharing and use". Journal of Knowledge Management. vol. 14, no. 1. pp. 128-140.

Hsieh, H. & Shannon, S. 2005. "Three Approaches to Qualitative Content Analysis". Qualitative Health Research. vol. 5, November. pp. 1277-1288.

Hurmelinna-Laukkanen, P. 2011. "Enabling collaborative innovation – knowledge protection for knowledge sharing". European Journal of Innovation Management. vol. 14, no. 3. pp. 303-321.

Husted, K., Michailova, S., Minbaeva, D.B. & Pedersen, T. 2012. "Knowledge-sharing hostility and governance mechanisms: an empirical test". Journal of Knowledge Management. vol. 16, no. 5. pp. 754-773.

Ifinedo, P. 2012. "Understanding information systems security policy compliance: An integration of the theory of planned behaviour and the protection motivation theory". Computers & Security. vol. 31, no. 1. pp. 83-95.

Ilvonen, I. 2010. “Knowledge Management and Knowledge Security–a Conceptual Comparison”. In Proceedings of the 9th European Conference on Information Warfare and Security: University of Macedonia and Strategy International Thessaloniki, Greece, 1-2 July 2010. Academic Conferences Limited.

Ipe, M. 2003. "Knowledge Sharing in Organizations: A Conceptual Framework". Human Resource Development Review. vol. 2, no. 4. pp. 337-359.

ISO/IEC. 2005.27001. Standard on Information Security Management Requirements.

Jarvenpaa, S.L. & Majchrzak, A. 2010. "Vigilant Interaction in Knowledge Collaboration: Challenges of Online User Participation Under Ambivalence". Information Systems Research. vol. 21, no. 4. pp. 773-784.

Jarzabkowski, P. & Spee, A. P. 2009. “Strategy-as-Practice: A review and future directions for the field”. International Journal of Management Reviews. vol. 11, no. 1. pp. 69-95.

Jauch, L.R., Osborn, R.N. & Martin, T.N. 1980. "Structured Content Analysis of Cases: A Complementary Method for Organizational Research". The Academy of Management Review. vol. 5, no. 4. pp. 517-525.

Jill, F.T. & Carroll, J. 2010. "Corporate Culture Narratives as the Performance of Organisational Meaning". Qualitative Research Journal. vol. 10, no. 1. pp. 28-39.

Johnson, G. & Scholes, K. 2002. Exploring Corporate Strategy. 6th ed. Pearson Education, Essex.

Johnston, A.C. & Warkentin, M. 2010. "Fear Appeals and Information Security Behaviours: an Empirical Study". MIS Quarterly. vol. 34, no. 3. pp. 549-566.

Kairab, S. 2005. A Practical Guide to Security Assessments. Auerbach, Boca Raton.

Kang, J., Rhee, M. & Kang, K.H. 2010. "Revisiting knowledge transfer: Effects of knowledge characteristics on organizational effort for knowledge transfer". Expert Systems with Applications. vol. 37, no. 12. pp. 8155-8160.

Kayworth, T. & Whitten, D. 2010. "Effective Information Security Requires a Balance of Social and Technology Factors". MIS Quarterly Executive. vol. 9, no. 3. pp. 163-175.

Ko, DG. 2010. "Consultant competence trust doesn't pay off, but benevolent trust does! Managing knowledge with care". Journal of Knowledge Management. vol. 14, no. 2. pp. 202-213.

Ko, DG. & Dennis, A.R. 2011. "Profiting from Knowledge Management: The Impact of Time and Experience". Information Systems Research. vol. 22, no. 1. pp. 134-152.

Kogut, B. & Zander, U. 1992. "Knowledge of the Firm, Combinative Capabilities, and the Replication of Technology". Organization Science. vol. 3, no. 3, Focused Issue: Management of Technology. pp. 383-397.

Kotler, P. 2000. Marketing Management. The Millennium Edition ed. Prentice Hall, Upper Saddle River, New Jersey.

Kumar, R.L., Park, S. & Subramaniam, C. 2008. "Understanding the Value of Countermeasure Portfolios in Information Systems Security". Journal of Management Information Systems. vol. 25, no. 2. pp. 241-279.

Lacey, D. 2010. "Understanding and transforming organizational security culture". Information Management & Computer Security. vol. 18, no. 1. pp. 4-13.

Liebeskind, J. 1997. "Keeping organizational secrets: protective institutional mechanisms and their costs". Industrial & Corporate Change. vol. 6, pp. 623-663.

Lindgren, R., Stenmark, D. & Ljungberg, J. 2003. "Rethinking competence systems for knowledge-based organizations". European Journal of Information Systems. vol. 12, no. 1. pp. 18-29.

Line, M.B. 1999. "Types of organisational culture". Library Management. vol. 20, no. 2. pp. 73-75.

Ling-Yee, L. 2011. "Marketing metrics' usage: Its predictors and implications for customer relationship management". Industrial Marketing Management. vol. 40, no. 1. pp. 139-148.

Lippman, S.A. & Rumelt, R.P. 1982. "Uncertain Imitability: An Analysis of Interfirm Differences in Efficiency under Competition". The Bell Journal of Economics. vol. 13, no. 2. pp. 418-438.

Lu, H. & Liu, B. 2009. "DFANS: A highly efficient strategy for automated trust negotiation". Computers & Security. vol. 28, no. 7. pp. 557-565.

Lucas, L.M. 2010. "The evolution of organizations and the development of appropriate knowledge structures". Journal of Knowledge Management. vol. 14, no. 2. pp. 190-201.

Ma, Z. & Yu, K. 2010. "Research paradigms of contemporary knowledge management studies: 1998-2007". Journal of Knowledge Management. vol. 14, no. 2. pp. 175-189.

Mäenpää, I. & Voutilainen, R. 2012. "Insurances for human capital risk management in SMEs". VINE: The journal of information and knowledge management systems. vol. 42, no. 1. pp. 52-66.

Maier, R. 2010. Knowledge Management Systems. 3rd ed. Springer-Verlag, Berlin.

Majchrzak, A. & Jarvenpaa, S.L. 2004. "Information security in cross-enterprise collaborative knowledge work". Emergence: Complexity & Organization. vol. 6, no. 4. pp. 40-50.

Mansfield, E. 1986. "Patents and innovation: an empirical study". Management Science. vol. 32, pp. 173-181.

Mansourian, Y. 2008. "Exploratory nature of, and uncertainty tolerance in, qualitative research". Qualitative research. vol. 109, no. 5. pp. 273-286.

Mantere, S. 2005. "Strategic practices as enablers and disablers of championing activity". Strategic Organization. vol. 3, no. 2. pp. 157-184.

Mantere, S. & Vaara, E. 2008. "On the Problem of Participation in Strategy: A Critical Discursive Perspective". Organization Science. vol. 19, no. 2. pp. 341-358.

Marshall, M.N. 1996. "Sampling for qualitative research". Family practice. vol. 13, no. 6. pp. 522-526.

Martin, J., Feldman, M.S., Hatch, M.J. & Sitkin, S.B. 1983. "The Uniqueness Paradox in Organizational Stories". Administrative Science Quarterly. vol. 28, no. 3, Organizational Culture. pp. 438-453.

Martins, A. & Eloff, J.H. 2002, "Information Security Culture", In Security in the information society IFIP/SEC2002Kluwer Academic Publishers, Boston, pp. 203.

Massingham, P. 2010. "Knowledge risk management: a framework". Journal of Knowledge Management. vol. 14, no. 3. pp. 464-485.

Maxwell, J.A. 1996. Qualitative Research Design: An Interactive Approach. Sage, Thousand Oaks.

McAdam, R., Mason, B. & McCrory, J. 2007. "Exploring the dichotomies within the tacit knowledge literature: towards a process of tacit knowing in organizations". Journal of Knowledge Management. vol. 11, no. 2. pp. 43-59.

McInerney, C.R. & Day, R.E.(. 2007. Rethinking knowledge managementfrom knowledge objects to knowledge processes. Springer, Berlin.

Metsämuuronen, J. 2005. Tutkimuksen tekemisen perusteet ihmistieteissä. 3rd ed. Gummerus Kirjapaino Oy, Jyväskylä. (In Finnish)

Milne, P. 2007. "Motivation, incentives and organisational culture". Journal of Knowledge Management. vol. 11, no. 6. pp. 28-38.

Ministry of Justice. 2012.Limited Liability Companies Act (osakeyhtiölaki). Finland.

Mookerjee, V., Mookerjee, R. & Bensoussan, A. 2011. "When Hackers Talk: Managing Information Security Under Variable Attack Rates and Knowledge Dissemination". Information Systems Research. vol. 22, no. 3. pp. 606-623.

Morgan, G. 2006. Images of Organization. Updated ed. Sage, Thousand Oaks.

Morse, J.M., Barrett, M., Mayan, M., Olson, K. & Spiers, J. 2008. "Verification strategies for establishing reliability and validity in qualitative research". International Journal of Qualitative Methods. vol. 1, no. 2. pp. 13-22.

Myers, M. 2000. "Qualitative research and the generalizability question: Standing firm with Proteus". The Qualitative Report [Online serial]. vol. 4, no. 1/2.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. & Vance, A. 2009. "What levels of moral reasoning and values explain adherence to information security rules? An empirical study". European Journal of Information Systems. vol. 18, no. 2 Special Issue: Behavioral and Policy Issues in Information. pp. 126-139.

Nahapiet, J. & Ghosal, S. 1998. "Social Capital, Intellectual Capital and the Organisational Advantage". Academy of Management Review. vol. 22, no. 2. pp. 243-266.

Nassimbeni, G., Sartor, M. & Dus, D. 2012. "Security risks in service offshoring and outsourcing". Industrial Management & Data Systems. vol. 112, no. 3. pp. 405-440.

Neef, D. 2005. "Managing corporate risk through better knowledge management". The Learning Organization. vol. 12, no. 2. pp. 112-124.

Nicholas, D. 2000. Assessing Information Needs: Tools, Techniques and Concepts for the Internet Age. 2nd ed. Aslib, London.

Niels, O.P. 2008. "Management tools, organisational culture and leadership: an explorative study". Performance Measurement and Metrics. vol. 9, no. 2. pp. 138-152.

Niiniluoto, I. 1984. Johdatus tieteenfilosofiaan. Käsitteen- ja teorianmuodostus. 2. ed. Otava, Helsinki. (In Finnish)

Niu, KH. 2010. "Organizational trust and knowledge obtaining in industrial clusters". Journal of Knowledge Management. vol. 14, no. 1. pp. 141-155.

Nold, H.A. 2012. "Linking knowledge processes with firm performance: organizational culture". Journal of Intellectual Capital. vol. 13, no. 1. pp. 16-38.

Nonaka, I. 1991. "The Knowledge-Creating Company". Harvard Business Review. vol. 69, no. 6. pp. 96-104.

Nonaka, I. 1994. "A Dynamic Theory of Organizational Knowledge Creation". Organization Science. vol. 5, no. 1. pp. pp. 14-37.

Nonaka, I. & Takeuchi, H. 1995. The Knowledge Creating Company. Oxford University Press, New York.

Nonaka, I., Toyama, R. & Konno, N. 2000. "SECI, Ba and Leadership: a Unified Model of Dynamic Knowledge Creation". Long range planning. vol. 33, no. 1. pp. 5-34.

Norman, P. 2001. "Are Your Secrets Safe? Knowledge Protection in Strategic Alliances". Business Horizons. vol. 44, no.6. pp. 51-60.

O'Donoghue, N. & Croasdell, D.T. 2009. "Protecting knowledge assets in multinational enterprises: a comparative case approach". VINE: The journal of information and knowledge management systems. vol. 39, no. 4. pp. 298-318.

Oguz, F. & Ayse, E.S. 2011. "Mystery of the unknown: revisiting tacit knowledge in the organizational literature". Journal of Knowledge Management. vol. 15, no. 3. pp. 445-461.

Olkkonen, T. 1993. Johdatus teollisuustalouden tutkimustyöhön. Helsinki University of Technology. Industrial Economics and Industrial Psychology. Report No. 152.

Paalumäki,A. 2010.Organisaatiokulttuuri tutkimusalueena. TTY Turvallisuuskulttuuriseminaari (A presentation at a safety culture seminar at TUT) 23.11.2010. (In Finnish)

Payne, A. & Holt, S. 1999. "A Review of the 'Value' Literature and Implications for Relationship Marketing". Australasian Marketing Journal (AMJ). vol. 7, no. 1. pp. 41-51.

Peltier, T.R., Peltier, J. & Blackley, J. 2005. Information security fundamentals. Auerbach Publications, Boca Raton.

Penrose, E. 1995. The Theory of the Growth of the Firm. 3rd ed. Oxford University Press, Oxford.

Pettigrew, A. M. 1979. “On Studying Organizational Cultures”. Administrative Science Quarterly. vol. 24, no. 4. pp. 570-581.

Poston, R.S. & Speier, C. 2005. "Effective use of Knowledge Management Systems: a Process Model of Content Ratings and Credibility Indicators". MIS Quarterly. vol. 29, no. 2. pp. 221-244.

Potter, C.C. 1989. "What is Culture: and Can it be Useful for Organisational Change Agents?". Leadership & Organization Development Journal. vol. 10, no. 3. pp. 17-24.

Prahalad, C.K. & Hamel, G. 1990. "The Core Competence of the Corporation". Harvard Business Review. vol. 68, no. 3. pp. 79-91.

Puusa, A. 2008. "Käsiteanalyysi tutkimusmenetelmänä". Premissi. no. 4. pp. 36-43. (In Finnish)

Quinn, J.B., Anderson, P. & Finkelstein, S. 1996. "Managing Professional Intellect: Making the Most of the Best". Harvard Business Review. vol. 74, no. 3-4. pp. 71-80.

Rai, R.K. 2011. "Knowledge management and organizational culture: a theoretical integrative framework". Journal of Knowledge Management. vol. 15, no. 5. pp. 779-801.

Randeree, E. 2006. "Knowledge management: securing the future". Journal of Knowledge Management. vol. 10, no. 4. pp. 145-156.

Rangachari, P. 2009. "Knowledge sharing networks in professional complex systems". Journal of Knowledge Management. vol. 13, no. 3. pp. 132-145.

Reiman,T. & Oedewald,P. 2010.Turvallisuuskulttuuri osana organisaatiokulttuuria. TTY Turvallisuuskulttuuriseminaari (Presentation at a safety culture seminar in TUT) 23.11.2010. (In Finnish)

Riege, A. 2005. "Three-dozen knowledge-sharing barriers managers must consider". Journal of Knowledge Management. vol. 9, no. 3. pp. 18-35.

Riivari, E. Lämsä, A-M. Kujala, J. Heiskanen, E. 2012. ”The ethical culture of organisations and organisational innovativeness”. European Journal of Innovation Management. vol. 15, no. 3. pp. 310-331.

Rodgers, B.L. 1989. "Concepts, analysis and the development of nursing knowledge: the evolutionary cycle". Journal of Advanced Nursing. vol. 14, pp. 330-345.

Ross, M.V. & Schulte, W.D. 2005. "Chapter 10 - Knowledge Management in a Military Enterprise: a Pilot Case Study of the Space and Warfare Systems Command" in

Creating the Discipline of Knowledge Management, ed. M. Stankosky, Butterworth-Heinemann, Boston, pp. 157-170.

Ruighaver, A.B., Maynard, S.B. & Chang, S. 2007. "Organisational security culture: Extending the end-user perspective". Computers & Security. vol. 26, no. 1. pp. 56-62.

Ryan, J.H. 2006a. "Knowledge management needs security too". VINE: The journal of information and knowledge management systems. vol. 36, no. 1. pp. 45-48.

Ryan, J.H. 2006b. "Managing knowledge security". VINE: The journal of information and knowledge management systems. vol. 36, no. 2. pp. 143-145.

Ryan, J.H. 2006c. "Political engineering in knowledge security". VINE: The journal of information and knowledge management systems. vol. 36, no. 3. pp. 265-266.

Sandhawalia, B.S. & Dalcher, D. 2011. "Developing knowledge management capabilities: a structured approach". Journal of Knowledge Management. vol. 15, no. 2. pp. 313-328.

Sanyal, P. 2004. "Intellectual property rights protection and location of R&D by multinational enterprises". Journal of Intellectual Capital. vol. 5, no. 1. pp. 59-76.

Saunders, M., Lewis, P. & Thornhill, A. 2009. Research Methods for Business Students. 5th ed. Prentice Hall, Harlow.

Scheepers, R., Venkitachalam, K. & Gibbs, M.R. 2004. "Knowledge strategy in organizations: refining the model of Hansen, Nohria and Tierney". The Journal of Strategic Information Systems. vol. 13, no. 3. pp. 201-222.

Schein, E. 1984. "Coming to a New Awareness of Organizational Culture". Sloan Management Review. vol. 25, no. 2. pp. 2-16.

Schiuma, G. 2012. "Managing knowledge for business performance improvement". Journal of Knowledge Management. vol. 16, no. 4. pp. 515-522.

Schlienger, T. & Teufel, S. 2003, "Analyzing information security culture: increased trust by an appropriate information security culture", Proceedings of the 14th International Workshop on Database and Expert Systems Applications, pp. 405.

Schofield, J.W. 2002, "Increasing the generalizability of qualitative research" in The Qualitative Researcher's Companion, eds. M. Huberman & M. Miles, Sage, London, pp. 171-204.

Schultze, U. & Leidner, D.E. 2002. "Studying Knowledge Management in Information Systems Research: Discourses and Theoretical Assumptions". MIS Quarterly. vol. 26, no. 3. pp. 213-242.

Seetharaman, A., Hadi Helmi Bin, Z.S. & A.S. Saravanan 2002. "Intellectual capital accounting and reporting in the knowledge economy". Journal of Intellectual Capital. vol. 3, no. 2. pp. 128-148.

Shedden, P., Scheepers, R. & Smith, W.:.A., A. 2011. "Incorporating a knowledge perspective into security risk assessments". VINE: The journal of information and knowledge management systems. vol. 41, no. 2. pp. 152-166.

Shorten, B. 2004, "Information Security Policies from the Ground Up" in Information Security Management Handbook, eds. H. Tipton & M. Krause, 5th ed, CRC Press, Boca Raton, pp. 917-924.

Sillanpää, V., Lönnqvist, A., Koskela, N., Koivula, U., Koivuaho, M. & Laihonen, H. 2010. "The role of intellectual capital in non-profit elderly care organizations". Journal of Intellectual Capital. vol. 11, no. 2. pp. 107-122.

Siponen, M. 2000. "A conceptual foundation for organizational information security awareness.". Information Management & Computer Security. vol. 8, no. 1. pp. 31-41.

Siponen, M. & Vance, A. 2010. "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations". MIS Quarterly. vol. 34, no. 3. pp. 487-502.

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. vol. 34, no. 3. pp. 463-486.

Spears, J.L. & Barki, H. 2010. "User Participation in Information Systems Security Risk Management". MIS Quarterly. vol. 34, no. 3. pp. 503-520.

Spender, J. 1996. "Making Knowledge the Basis of a Dynamic Theory of the Firm". Strategic Management Journal. vol. 17, no. Winter Special Issue. pp. 45-62.

Stantona, J.M., Stama, K.R., Mastrangelo, P. & Joiton, J. 2005. "Analysis of end user security behaviors". Computers & Security. vol. 24, no. 2. pp. 124-133.

Suppiah, V. & Manjit, S.S. 2011. "Organisational culture's influence on tacit knowledge-sharing behaviour". Journal of Knowledge Management. vol. 15, no. 3. pp. 462-477.

Swart, J. & Harvey, P. 2011. "Identifying knowledge boundaries: the case of networked projects". Journal of Knowledge Management. vol. 15, no. 5. pp. 703-721.

Taleb, N.N. 2008. The Black Swan - the impact of the highly improbable. Penguin, London.

The American Heritage Dictionary of the English Language. 2009. 4th ed. Houghton Mifflin Company.

Thierauf, R. 2001. Effective Business Intelligence Systems. Quorum Books, Westport.

Thomson, K., von Solms, R. & Louw, L. 2006. "Cultivating an organizational information security culture". Computer Fraud & Security. vol. 2006, no. 10. pp. 7-11.

Tipton, H. & Krause, M. (eds) 2004, Information security management handbook, 5th ed, CRC Press, Boca Raton.

Tranfield, D., Denyer, D. & Palminder, S. 2003. "Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of systematic Review". British Journal of Management. vol. 14, no. 3. pp. 207-222.

Tsohou, A., Karyda, M., Kokolakis, S. & Kiountouzis, E. 2010. "Aligning Security Awareness with Information Systems Security Management". Journal of Information System Security. vol. 6, no. 1. pp. 36-54.

Tsohou, A., Kokolakis, S., Karyda, M. & Kiountouzis, E. 2008. "Investigating Information Security Awareness: Research and Practice Gaps". Information Security Journal: A Global Perspective. vol. 17, no. 5. pp. 207-227.

Tsoukas, H. 2003, "Do we really understand tacit knowledge?" in The Blackwell Handbook of Organizational Learning and Knowledge Management, eds. Easterby-Smith, M. & Lyles, M.A. Blackwell, Oxford, pp. 410-427.

VAHTI. 2009.VAHTI 05/2009 Effective Information Security. Information security instructions to public organizations by ministry of finance. Helsinki.

van den Hooff, B., Schouten, A. P., & Simonovski, S. 2012. “What one feels and what one knows: the influence of emotions on attitudes and intentions towards knowledge sharing”. Journal of Knowledge Management, vol. 16, no. 1, pp. 148-158.

Van Niekerk, J.F. & Von Solms, R. 2010. "Information security culture: A management perspective". Computers & Security. vol. 29, no. 4. pp. 476-486.

Vedder, R., Vanecek, M., Guynes, C.S. & Cappel, J. 1999. "CEO and CIO Perspectives on Competitive Intelligence". Communications of the ACM. vol. 42, no. 8. pp. 109-116.

Vitt, E., Luckevich, M. & Misner, S. 2002. Business Intelligence: Making Better Decisions Faster. Microsoft Press, Washington.

von Krogh, G. 2009. "Individualist and collectivist perspectives on knowledge in organizations: Implications for information systems research". Journal of Strategic Information Systems. vol. 18, pp. 119-129.

von Krogh, G., Nonaka, I. & Aben, M. 2001. "Making the Most of Your Company’s Knowledge: Strategic Framework". Long Range Planning. vol. 34, pp. 421-439.

von Solms, B. 2000. "Information Security - The Third Wave? ". Computers & Security. vol. 19, pp. 615-620.

von Solms, B. & von Solms, R. 2004a. "The 10 deadly sins of information security management". Computers & Security. vol. 23, no. 5. pp. 371-376.

von Solms, R. & von Solms, B. 2004b. "From policies to culture". Computers & Security. vol. 23, no. 4. pp. 275-279.

Vuori, V. & Okkonen, J. 2012. "Refining information and knowledge by social media applications: Adding value by insight". VINE: The journal of information and knowledge management systems. vol. 42, no. 1. pp. 117-128.

Wang, J., Chaudhury, A. & Rao, H.R. 2008. "A Value-at-Risk Approach to Information Security Investment". Information Systems Research. vol. 19, no. 1. pp. 106-120.

Weber, R. 1990. Basic Content Analysis. 2nd ed. Sage, London.

Webster, J. & Watson, R.T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review". MIS Quarterly. vol. 26, no. 2. pp. xiii-xxiii.

Werlinger, R., Hawkey, K. & Beznosov, K. 2009. "An integrated view of human, organizational, and technological challenges of IT security management". Information Management & Computer Security. vol. 17, no. 1. pp. 4-19.

Wernerfelt, B. 1984. "A Resource-Based View of the Firm". Strategic Management Journal. vol. 5, no. 2. pp. 171-180.

Whetten, D.A. 1989. "What constitutes a theoretical contribution?". Academy of Management Review. vol. 14, no. 4. pp. 490-495.

Whitman, M.E. & Mattord, H.J. 2003. Principles of information security. Course Technology, Canada.

Wilkins, J., van Wegen, B. & de Hoog, R. 1997. "Understanding and Valuing Knowledge assets: Overview and Method". Expert Systems with Applications. vol. 13, no. 1. pp. 55-72.

Willem, A., Buelens, M. & Scarbrough, H. 2006. "The role of inter-unit coordination mechanisms in knowledge sharing: a case study of a British MNC". Journal of Information Science. vol. 32, no. 6. pp. 539-561.

Wilson, J. 1963. Thinking with concepts. Repr. ed. Cambidge University Press, New York.

Wilson, T.D. 1994. "Tools for the analysis of business information needs". Aslib Proceedings. vol. 46, no. 1. pp. 19-23.

Xi, Y. & Dang, Y. 2007. "Method to Analyze Robustness of Knowledge Network based on Weighted Supernetwork Model and Its Application". Systems Engineering - Theory & Practice. vol. 27, no. 4. pp. 134-140.

Yin, R.K. 1994. Case study researh - Design and methods. 2nd ed. Sage, Newbury Park.

Zhang, Z. & Sundaresan, S. 2010. "Knowledge markets in firms: knowledge sharing with trust and signalling". Knowledge Management Research and Practice. vol. 8, no. 4. pp. 322-339.

APPENDIX 1. Interview questions used in the introductory empirical study

Taustatietoa

1. Yrityksen toiminnan lyhyt kuvaus (toimiala, asiakkaat, toimittajat)
2. Tilojen kuvaus (mm. toimistoympäristö, tuotantolaitteet, onko jaettu muiden yritysten kanssa?)
3. Työntekijöiden määrä yrityksessä
4. Mitä tietoturvallisuus on?
5. Minkälaista tietoa yrityksessä käsitellään? Mikä tieto yritykselle on tärkeää?
6. Mitä toimintoja yrityksessä on ulkoistettu (esim. siivous, vartiointi, IT-palvelut – nimeä palveluiden tarjoaja)?
7. Onko yrityksellä tietoturvallisuuteen liittyviä sertifikaatteja? (ISO 9001, ISO 17799 tai ISO 27001, ISO 18045, CMM, BSI, WebTrust tms.).
8. Onko yrityksen arvot määritelty? Onko arvoissa tai niitä selittävässä dokumentaatiossa viittauksia tietoturvallisuuden arvoihin eli tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen?

Hallinnollinen turvallisuus

9. Kuvaile tietoturvallisuuspolitiikkaanne (tavoitteet, laajuus, onko dokumentoitu?). Millaisella dokumenttikokonaisuudella tietoturvallisuutta hallitaan, ts. onko eri osa-alueille muodostettu omaa tietoturvallisuuspolitiikkaa (esim. yleinen tietoturvallisuuspolitiikka, verkon tietoturvallisuus-politiikka jne.)?
10. Miten vastuu tietoturvallisuudesta on jaettu eri organisaatiotasoille? Kuinka tietoturvallisuusvastuista viestitään? Kuinka työntekijät tietävät omat tietoturvallisuusvastuunsa?
11. Järjestetäänkö yrityksessä sisäistä tietoturvallisuuden arviointia? Kuinka usein? Kuka arvioi, ja miten arviointi tehdään?
12. Valvotaanko tietoturvallisuuspolitiikan tai -ohjeistusten noudattamista? Miten?

Henkilöstöturvallisuus

13. Miten yrityksessä kehitetään tietoturvallisuustietoisuutta, eli henkilökunnan asenteita ja motivaatiota tietoturvallisuutta kohtaan?
14. Miten työntekijöitä koulutetaan tietoturvallisuuteen liittyvissä asioissa? Onko uusille työntekijöille olemassa valmista koulutuspakettia tai ohjeistusta (esim. heti rekrytoinnin jälkeen)? Jos henkilöstöä ei kouluteta, mitkä ovat suurimmat syyt siihen?
15. Kuinka työntekijöiden taustat selvitetään rekrytointitilanteessa (rikosrekisteri, suosittelijoiden lausunnot yms.)? Minkälaisia riskejä rekrytointiin yrityksen mielestä liittyy?
16. Millaisia turvallisuusmääräyksiä ja ehtoja kirjataan työsopimuksiin?
17. Onko työntekijöillä mahdollisuus etätyöskentelyyn? Kuinka etätyöskentely on hoidettu?
18. Onko yrityksessä dokumentoituja tai muuten vakiintuneita toimintatapoja työsuhteen päättyessä (pääsy/käyttöoikeuksien hallinta, työhön liittyvän materiaalin luovutus)?

Ohjelmisto-, laitteisto-, ja tietoliikenteen turvallisuus

19. Onko työntekijöillä oikeus asentaa ohjelmia tietokoneilleen? Miten käytössä olevien ohjelmien ylläpito on organisoitu?
20. Mitä siirrettäviä medioita yrityksessä on lupa käyttää (esim. USB-muistit, CD, DVD)? Onko siirrettäviä medioita suojattu luvattomalta pääsyltä, väärinkäytöltä tai muuttumiselta? Miten? Millä tavalla niiden käyttöön ohjeistetaan?
21. Onko kannettavien tietokoneiden kovalevyjä salattu? Jos ei, niin miksi? Minkälaista tietoa kannettavilla välineillä käytetään?
22. Kuinka virustarkastus on organisoitu yrityksessä (esim. päivitykset, automaattitarkastukset)?
23. Minkälaisia menetelmiä yrityksessä käytetään tietoliikenteen salaamiseen (esim. sähköpostin salausohjelmat, etäyhteydet)? Valvotaanko näiden käyttöä?
24. Kuinka käyttäjien autentikointi (oikeaksi tunnistaminen) ulkopuolisista yhteyksistä on järjestetty?

Fyysinen turvallisuus

25. Onko toimitiloissa kulunvalvontajärjestelmä? Minkälainen? Kuinka toimitilan kulkuoikeudet ja -säännöt on määritelty? Käytetäänkö videovalvontaa, miten?
26. Onko henkilökunnalla kuvallisia henkilökortteja ja väliaikaisia kortteja vierailijoille? Jos ei, miten yrityksessä tunnistetaan henkilökunta ja vierailijat? Onko yrityksessä määritelty sääntöjä vierailijoita koskien?
27. Kuinka pääsy tietoturvallisuuden kannalta merkittäviin paikkoihin on järjestetty (esim. palvelinhuone, arkistotilat, muut yritykselle tärkeän tiedon kannalta kriittiset tilat)?
28. Kuinka tulipalon ja vesivahingon tunnistus, hälytys ja torjunta on järjestetty?

Tietoaineisto- ja käyttöturvallisuus

29. Onko yrityksessä määritelty politiikka tietojärjestelmiin pääsylle? (esim. käytetäänkö henkilökohtaista käyttäjätunnusta ja salasanaa? Miten pääsyoikeudet määritellään?)
30. Minkälainen salasanapolitiikka yrityksessä on? Miten sen noudattamista valvotaan?
31. Kuinka tieto on luokiteltu (luokittelulutapa, kuinka käsitellään, hävittäminen jne.)? Onko lajittelutapa dokumentoitu?
32. Onko työntekijöiden pääsyoikeuksia rajoitettu vain heidän työtehtävissään tarvitsemiin tietoihin? Onko henkilöstön tehtävien jaossa kiinnitetty huomiota turvattomiin/vaarallisiin työyhdistelmiin?
33. Onko tiedoilla ja tietojärjestelmillä nimetty vastuuhenkilö? (tiedon/järjestelmän omistaja). Jos vastuuhenkilöä ei ole, kuvaile korvaavia toimintatapoja.
34. Minkälainen varmuuskopiointipolitiikka yrityksessä on? Miten varmuuskopiointi on käytännössä organisoitu? Missä varmuuskopioita säilytetään?

Liiketoiminnan jatkuvuus ja riskienhallinta

35. Millä tavalla yrityksessä arvioidaan tietoturvallisuuteen liittyviä riskejä? Kuka niitä arvioi? Kuinka usein?
36. Kuvaile menettelytapoja liiketoiminnan jatkuvuuden varmistamiseksi ongelma/häiriötilanteissa (esim. liiketoiminnan jatkuvuussuunnitelma, suunnitelma onnettomuustilanteista selviämiseksi, onko

varahenkilöitä avainhenkilöiden tilalle) Miten toimitaan, jos toimitiloissa tapahtuu tulipalo? Kuka tekee mitäkin?

37. Käytetäänkö agenttien, jällenmyyjien, alihankkijoiden tai yhteistyökumppaneiden kanssa salassapitosopimuksia (non-disclosure agreement)? Miten tiedonvaihto yhteistyökumppanien kanssa tapahtuu? Onko yhteistyökumppanien kanssa ollut ongelmia tietoturvallisuuteen liittyen? Minkälaisia?
38. Miten yrityksenne käsityksestä tietoturvallisuudesta viestitään asiakkaille ja toimittajille? Onko tietoturvallisuus markkinointitekijä yritykselle?

APPENDIX 2. Interview themes used in the primary empirical study

Haastatteluteemat

Ensimmäinen osa, avoin keskustelu

Tietämyksestä

- arvokas tietämys
- miten arvokas tietämys tunnistetaan, kuka sen tunnistaa?
- uhat tietämystä kohtaan

Tietämyksenhallinta ja tietämysturvallisuus

- tietämyksen hallinnan periaatteita
- tietämyksenhallinnan ja turvallisuuden roolit, ristiriidat/yhteistyön teemat

Toinen osa, tarkentavat teemat

Tietämyksen turvaamisen käytännöt

- tietämyksen turvaamisen ohjeistus vs. tietoturvallisuuden ohjeistukset
- turvallinen käyttäytyminen (tiedon suhteen) ja sen ohjeistukset
- tietämyksen jakamisen käytännöt ja ohjeistus
- tietämyksen jakamiseen asennoituminen: jaetaanko vai pidetäänkö omana tietona
- tietämyksen jakamisen välineet ja ohjeistus
- muutokset tietämyksen jakamisessa
- avaukset tietämyksen turvaamiseksi
- tietämyksen luokittelu ja sen välineet

Käsitteet (alateemoja, tarkennetaan lopuksi mikäli tarpeen)

- tietämyksen turvaamisen ja hallinnan yhteydessä käytettävät käsitteet (suomeksi ja englanniksi, mikäli työkielenä)
- tietämyksen käsite työyhteisössä

Tampereen teknillinen yliopisto
PL 527
33101 Tampere

Tampere University of Technology
P.O.B. 527
FI-33101 Tampere, Finland

ISBN 978-952-15-3186-6
ISSN 1459-2045