TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

Elina Niemimaa

Crafting Organizational Information Security Policies

Julkaisu 1507 • Publication 1507

Tampere 2017

Tampereen teknillinen yliopisto. Julkaisu 1507
Tampere University of Technology. Publication 1507

Elina Niemimaa

Crafting Organizational Information Security Policies

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 18th of November 2017, at 12 noon.

Tampereen teknillinen yliopisto - Tampere University of Technology
Tampere 2017

Doctoral candidate:
Elina Niemimaa
Industrial and Information Management
Business and Built Environment
Tampere University of Technology
Finland

Supervisor:
Professor Nina Helander
Industrial and Information Management
Business and Built Environment
Tampere University of Technology
Finland

Pre-examiners:
Professor Carol Hsu
School of Economics and Management
Tongji University
China

Professor Karin Hedström
School of Business
Örebro University
Sweden

Opponent:
Professor Pia Hurmelinna-Laukkanen
Management and International Business
University of Oulu
Finland

ISBN 978-952-15-4037-0 (printed)
ISBN 978-952-15-4053-0 (PDF)
ISSN 1459-2045

ABSTRACT

An organizational information security policy (InfoSec policy) is a direction-giving instrument for information security within an organization that seeks to communicate an organization's posture in protecting its information assets. Researchers and practitioners alike agree that an InfoSec policy has a foundational role in securing an organization's information assets. In an era where information is a precious resource and information security breaches are ever more prevalent, developing such a policy has become even more crucial for organizations.

The importance of an InfoSec policy has resulted in scholarly research on the policy's contents and structure, and on the means to promote employee compliance to the set policies. In regards to policy development, research has privileged abstractions – abstract methods and procedures policy development should follow. By emphasizing such abstractions, research has paid less attention to how policies are crafted in practice.

Therefore, the purpose of this dissertation, which consists of a compendium of articles, is to increase our understanding of the crafting of InfoSec policies. Theoretically, the dissertation draws on practice theory, which takes orderly social and materially mediated doings and sayings ("practices") as an arena for studying organizational phenomena. Empirically, the dissertation includes three qualitative studies: two ethnographic studies on InfoSec policy crafting and one case study on the implications of the crafting to policy compliance. Empirical material includes participant and non-participant observation, documentary sources, and semi-structured interviews.

The dissertation contributes to the literature on information security management. The primary contribution of this dissertation is the conceptualization of InfoSec policy crafting as emerging in the lived contradictions between the international information security best practices and the local organizational practices. More broadly, the dissertation contributes to research on InfoSec policy development by positing that to understand policy crafting requires deep engagement with the actors who participate in the policy crafting and with the field where the policy is crafted. Further, the dissertation contributes to discussions on policy compliance by suggesting that compliance should be considered as partly emerging from and through the practices of the policy crafting and as relational to them. The potential for developing the policy as a joint engagement with different organizational members should not be underestimated.

The argument developed in this dissertation is that both organizations and

research should place more emphasis on the practical accomplishment of InfoSec policy crafting. InfoSec policy development is not about following a rote procedure, but is a practical, joined, and skilled accomplishment – a craft. Policy crafting influences what is included in and excluded from the policy and how the policy will be complied with.

TIIVISTELMÄ

Organisaation tietoturvapolitiikka on organisaation tietoturvaa ohjaava väline, joka pyrkii kommunikoimaan organisaation näkemyksen sen tietopääomien turvaamisesta. Tutkijat ja tietoturva-ammattilaiset ovat yhtä mieltä siitä, että tällainen tietoturvapolitiikka muodostaa organisaation tietoturvallisuuden perustan. Tietoturvapolitiikan muodostaminen on yhä tärkeämpää organisaatioille, koska organisaatiot ovat yhä riippuvaisempia tietopääomistaan ja koska näihin pääomiin kohdistuu yhä enemmän riskejä.

Tietoturvapolitiikan merkitys organisaatioille on synnyttänyt tutkimuskirjallisuutta tietoturvapolitiikan sisällöstä ja rakenteesta ja tavoista motivoida työntekijöitä noudattamaan organisaation politiikkaa. Politiikan muodostamisen osa-alueella, tutkimuskirjallisuus on keskittynyt korkeantason malleihin ja menetelmiin, joita politiikan muodostamisen pitäisi noudattaa. Keskittyessään tällaisiin malleihin ja menetelmiin, tutkimuskirjallisuus on jättänyt vähemmälle huomioille sen miten politiikka käytännössä tehdään.

Tämän väitöskirjatutkimuksen tarkoituksena onkin kasvattaa ymmärrystä tietoturvapolitiikkojen käytännön tekemisestä. Teoreettisesti väitöskirja ammentaa käytäntöteoreettisista lähtökohdista (engl. practice theory), joiden mukaan sosiaaliset käytännöt ovat keskeisiä organisaatioilmiöiden ymmärtämiselle. Empiirisesti väitöskirja koostuu kolmesta laadullisesta tutkimuksesta: kahdesta etnografisesta tutkimuksesta, joissa tarkastellaan tietoturvapolitiikan tekemistä ja yhdestä tapaustutkimuksesta, joka keskittyy politiikan tekemisen vaikutuksiin politiikalla saavutettaville lopputuloksille. Empiirinen aineisto koostuu osallistuvasta ja ei-osallistuvasta havainnoinnista, dokumenttilähteistä ja puolistrukturoiduista haastatteluista.

Väitöskirja kontribuoi tietoturvajohtamisen kirjallisuuteen. Väitöskirjan ensisijaisena kontribuutiona voidaan pitää tietoturvapolitiikan tekemisen käsitteellistämistä tekemiseksi, joka nousee tietoturvallisuuden parhaiden käytäntöjen ja organisaation käytäntöjen välisistä, eletyistä ristiriidoista. Laajemmin nähtynä tutkimus laajentaa kirjallisuutta, joka käsittelee politiikan muodostamista, esittämällä että politiikan tekemisen ymmärtäminen edellyttää syvää sitoutumista politiikan tekemiseen liittyviin ihmisiin ja kontekstiin. Lisäksi, tutkimus kontribuoi tietoturvapolitiikan noudattamista tutkivaan kirjallisuuteen esittämällä, että politiikan noudattaminen syntyy osittain politiikan teon käytännöistä ja käytännöissä sekä on suhteellinen näihin käytäntöihin nähden. Mahdollisuuksia, jotka politiikan tekeminen yhteistyössä organisaation eri

ihmisten kanssa tuo mukanaan ei pidäkään väheksyä.

Väitöskirjan keskeinen väite on, että organisaatioiden ja tutkimuskirjallisuuden tulisi keskittyä enemmän tietoturvapolitiikan käytännön tekemiseen. Politiikan muodostaminen ei ole jonkin ennalta määrätyn mallin tai kaavan noudattamista vaan käytännöllinen, osallistava ja ammattitaitoinen saavutus. Politiikan tekeminen vaikuttaa siihen mitä politiikkaan sisällytetään tai mitä siitä jätetään pois sekä siihen miten politiikkaa noudatetaan.

ACKNOWLEDGEMENTS

Nothing creative is ever created independently from the particular circumstances and people involved. Crafting a dissertation is by no means an exception. It benefits from encounters with curious and open minded people and from engaging in a dialog with them. Those encounters might be in person but as well they might be encounters with particularly inspiring work or writings of others. I wish to express my gratitude to everyone with whom I have had the chance to engage in a dialogue during my journey of crafting this dissertation.

I am most grateful to professor Carol Hsu and professor Karin Hedström for the honor of agreeing to review this dissertation. I sincerely admire their work and expertise on information security management research. Carol Hsu's work inspired me already when I was writing my master's thesis. Further, I would like to thank professor Pia Hurmelinna-Laukkanen for agreeing to be my esteemed opponent.

In addition, I would like to express my gratitude to my supervisors, professor Nina Helander, for helping me in finalizing this dissertation, and president of Tampere University of Technology, Mika Hannula, for his supportive and positive attitude and for giving me the freedom to conduct this research in my own way and on my own phase.

As of institutions I have previously studied, I would like to mention Luleå University of Technology and a very particular academic orientation of its MSc. in information security students and the supportive yet demanding teaching of associate professor Dan Harnesk and researcher John Lindström. Moreover, I am in greatly in debt to Turku Vocational Institute (Juhannuskukkula!) for providing me with a solid basis for whatever I want to study in my life.

I would also like to thank my colleagues Jari Närhi, Pauli Kauppila, Jyrki Nivala and Mika Tolvanen for giving me the opportunity to find a balance between my daily work as a consultant and my evening work as a researcher. Further, I thank Pauli and Jyrki and Secrays for making this dissertation financially possible.

This dissertation would have not been possible without the people and organizations with whom and in which I observed information security policy crafting.

I want to thank all my friends and family for being there for me during this journey. I feel have neglected you too many times, but, now, it is your time.

And last, I want to express my deepest gratitude to my dear friend, and life partner, Marko, how has engaged in a dialog with me throughout this journey.

3 October 2017
Elina Niemimaa

Table of contents

List of figures

List of tables

List of publications

This dissertation is based on the following original publications, which are referred to in the text as I–V. The publications are reproduced with the kind permission of the publishers in
Appendix B: Publications.

I Niemimaa, E. & Niemimaa, M. 2017, 'Information systems security policy implementation in practice: from best practices to situated practices', *European Journal of Information Systems*, vol. 25, no. 1, pp. 1–20.

II Niemimaa, E. 2016, 'Crafting an information security policy: insights from an ethnographic study', *Proceedings of the 37th International Conference on Information Systems (ICIS 2016)*, pp. 1–16.

III Niemimaa, E. 2016, 'Legitimising information security policy during policy crafting: exploring legimitising strategies', *Proceedings of the 27th Australian Conference on Information Systems (ACIS 2016)*, pp. 1–11.

IV Niemimaa, E. 2016, 'A practice lens for understanding the organizational and social challenges of information security management', *Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS 2016)*, paper 58.

V Niemimaa, M. & Laaksonen, A. E. 2015, 'Enacting information security policies in practice: three modes of policy compliance', in F.-X. de Vaujany, N. Mitev, G. F. Lanzara & A. Mukherjee (eds.), *Materiality, Rules and Regulation: New Trends in Management and Organization Studies*, Palgrave Macmillan.

Table 1 describes the author's contribution to each of the publications.

Table 1: Author's contribution in each publication

Publication	**Contribution**	**Publication forum rating for the publication channel**
Publication I: Information systems security policy implementation in practice: from best practices to situated practices (Niemimaa & Niemimaa, 2017)	Study design, data collection, and data analysis alone. Theorizing together with the second author of the paper. Main author for the following sections of the paper: Introduction, Theoretical background, Research approach, Ethnographic description of ISS policy project, and Translating a global ISS practice to situated practices. Discussion and Conclusion sections were written together with the second author of the paper.	3
Publication II: Crafting an information security policy: insights from an ethnographic study (Niemimaa, E. 2016)	Whole paper.	2
Publication III: Legitimising information security policy during policy crafting: exploring legimitising strategies (Niemimaa, 2016)	Whole paper.	1
Publication IV: A practice lens for understanding the organizational and social challenges of information security management (Niemimaa, 2016)	Whole paper.	1
Publication V: Enacting information security policies in practice: three modes of policy compliance (Niemimaa & Niemimaa, 2015) (Maiden name Laaksonen)	Study design, data collection, data analysis, and theorizing together with the other author of the paper. Main author for the following sections of the paper: Information security policy compliance (i.e., a part of the Theoretical background section), Research setting and methods, and Findings: sociomaterial practices of information security policy compliance. Participated in drafting other parts of the paper. The first author of the paper contributed significantly to the theoretical lens (i.e., sociomateriality) of the paper.	3

1 INTRODUCTION

1.1 Motivation and background

Information security refers to the preservation of confidentiality, integrity, and availability of information (ISO/IEC, 2014). Information leakages, breaches of confidential information, and intrusions into information systems are examples of information security issues that disturb organizational life and put organizations' information assets at risk. The average cost of information security breaches reached record levels in year 2015 (i.e., $3.79 million; Ponemon Institute, 2015). An industry survey reported that 76% of respondent organizations have already had or expect to have an information security breach that results in the loss of customers or business partners (Ponemon Institute, 2013). Examples of information security breaches and their high organizational impact abound in popular media. Therefore, it is no wonder that information security management is a top concern for organizations (Kappelman et al., 2016).

Both scholars and practitioners agree that an organizational information security policy (hereafter InfoSec policy) is central for organizations' efforts to secure their information assets. An InfoSec policy defines the "management direction and support for information security in accordance with business requirements and relevant laws and regulations" (ISO/IEC, 2013a, p. 25). Typically, it further defines an organization's information security goals and practices as well as the roles and responsibilities. Therefore, it is a direction-giving document (Höne & Eloff, 2002a) and the foundation of an organization's information security (e.g., Siponen & Iivari, 2006; Warkentin & Johnston, 2008; Doherty et al., 2009).

Acknowledging the foundational role of the InfoSec policy for organizations, research has studied the policy's structure (Baskerville & Siponen, 2002; Warkentin & Johnston, 2008), content (Höne & Eloff, 2002b; Siponen & Iivari, 2006), and delineated general and abstract methods for policy development (e.g., Rees et al., 2003; Whitman, 2008; Knapp et al., 2009; Flowerday & Tuyikeze, 2016). Research has further focused on what should take place after the policy has been developed; it is not sufficient to merely develop a policy, but the organization should comply with the set policy. In particular, researchers have studied employees' intention to comply with the policies (Warkentin & Willison, 2009) and the proposed antecedents of employees' compliant and non-compliant policy behavior (e.g., Siponen & Vance, 2010; Warkentin et al., 2011; Vance et al., 2012; Ifinedo, 2014; Hsu et al., 2015; Lowry & Moody, 2015). However, what is actually done in accomplishing an InfoSec policy in a given social, organizational, and material context has received less attention.

In the same vein, information security management standards (e.g., ISO/IEC27001; NIST SP-800) and other practitioner-oriented "best practice" guidelines prescribe an organization to formulate an InfoSec policy, but offer little in terms of how policy is accomplished in practice (Siponen, 2006). For example, one international information security management standard, ISO/IEC27001, requires organizations to establish an InfoSec policy that is "compatible with the strategic direction of the organization" (ISO/IEC, 2013a, p. 2). It further requires that the policy is appropriate for the organization, includes information security objectives or directs how such objectives are set, and entails a "commitment to satisfy applicable requirements related to information security" and a commitment to continually improve the organization's information security management (ISO/IEC, 2013a, p. 2). Unfortunately, the accompanying implementation guide, ISO/IEC27002 standard, is not anymore informative as it only describes the issues the policy should address.

It seems that, essentially, both scholarly contributions and practitioner-oriented literature are primarily concerned with the questions of *what*, while abstracting from the question of *how* InfoSec policy is accomplished in certain contexts. As Straub et al. (2008) argue "[n]ot only are the policies that protect this information much less frequently discussed, but the processes that lead to effective policies are even less favored by scientists and practitioners" (p. 6). Flowerday and Tuyikeze, (2016) echo them by summarizing: "The existing literature concentrates on describing the structure and content of a security policy, but fails, in general, to describe in detail the processes for developing the policy" (p. 170). Consequently, to use a metaphor, the literature on InfoSec policies and practitioner-oriented information security standards and best practices are like maps that guide practitioners on their journeys of developing InfoSec policies in organizations, but conceal all the decisions, internal disputes, changing conditions, and the unavoidable inaccuracies of the map. The actual journey carried out on the ground, nevertheless, requires understanding the terrain with all its peculiarities and changing conditions, as well as a compass and navigation skills; it requires ascending from the abstractions of the map to the actual situations and circumstances. The more complicated the journey, the more the map, while potentially useful by itself, hides what it actually takes to make the journey (Brown & Duguid, 1991).

In my work as an information security consultant, I have repeatedly witnessed the challenges that arise when the map fails to guide or provides misplaced information, and when ingenuity and innovative maneuvering are needed to overcome the peculiarities and changing conditions of developing an InfoSec policy. Among others, a key challenge of developing an InfoSec policy concerns developing a policy that reflects the organization's business or function, its inner workings, and context, as well as specific information security risks. Oftentimes, policies from two or more organizations, even across industries, are surprisingly similar; so similar that it is difficult to see how the policies reflect and are appropriately suited for the given organization. If the policies are more similar than not, how can they address the specific risks of the given organization?

Another challenge concerns the tension involved in developing a policy that addresses the specific needs of the organization, and which ensures that the policy will be implicated in organizational practices and organizing. Both during and after policy development, organizational members may see it as an unnecessary disturbance to organizational life or as something that is only of interest for the information security professionals. While such is often disregarded as organizational members' inadequate commitment to the InfoSec policy, in my experience, it may not be so much about commitment but of not understanding the reasons for having the policy in the first place. Employees and managers are perhaps dazed simply because they do not know how the policy took the shape it did and why it instructs them to do what it does. Despite the causes, the end result is often that information security professionals upload the policy to the organization's intranet, where it is as one interviewed business manager in this study metaphorically expressed: "*if you say that it's on the intranet then it's like you would say that it's on a sea.*"

While other means of policy implementation may take place, the end result of developing the policy is frequently that it is soon forgotten. Information security professionals may adduce policies in support of claiming high standards of information security during times of internal or external information security audits. Business managers and the like seldom encounter policies in their work. Policies remain decoupled from organizational practices (cf. Bromley & Powell, 2012; Dick, 2015). More often than not, the policy has only little effect on the organization (Karyda et al., 2005) – policy is not translated into organizational practice and complied with (Dhillon, 2007).

Given the above discussion, it would seem that, when carried out on the ground, the journey of InfoSec policy development appears as InfoSec policy crafting. According to Merriam-Webster's dictionary, the verb "to craft" means "to make or produce with care, skill, or ingenuity" (Merriam-Webster, 2017). In business strategy literature, Mintzberg (1987) portrayed the picture of someone crafting a strategy and argued that the crafting image captures how effective strategies come to be: "[f]ormulation and implementation merge into a fluid process of learning through which creative strategies evolve" (p. 66). Whereas formulation and development give rise to a rather mechanistic image of the InfoSec policy development as a process that actors should learn and follow, crafting pictures how InfoSec policy comes into being as an emergent and situated process, and through involvement and commitment. It appears as a practical accomplishment. Thus, in this dissertation, InfoSec policy development is analyzed as InfoSec policy crafting. InfoSec policy crafting refers to an emergent, exploratory, collaborative, and flexible, practical accomplishment through which an organization's InfoSec policy evolves in the flow of organizational practices.

Increasingly, authors writing about InfoSec policies have called for more attention to the question of *how* InfoSec policy is practically accomplished in certain contexts. This stream of research suggests that InfoSec policy crafting may be shaped by power relations (Lapke & Dhillon, 2008; Inglesant & Sasse, 2011), social structures (Nasution & Dhillon, 2012), or by various contextual factors such as the organizational structure and culture (Karyda et al., 2005). The policy itself is further subject to various, sometimes contradictory views of different stakeholders (Njenga & Brown, 2012; Niemimaa et al., 2013). While these authors write from different perspectives, they seem to agree about the need to complement the InfoSec policy development methods and discussions on InfoSec policy contents and structure (i.e., the *what* of InfoSec policies) with approaches which are more practice oriented, more sensitive to the power conflicts, and more sensitive to the contextual conditions of policy crafting more broadly. By doing so, they relate to a broader concern in management and organization studies: "attention to ordinary managerial activity in its processual, material, relational and historical iterations has often been missing, or reduced to and substituted by abstract categories" (Korica et al., 2017, p. 151). To begin to address this concern, management and organization studies have increasingly turned to studying situated management practices (e.g., Jarzabkowski & Spee, 2009; Miettinen et al., 2009; Smets et al., 2012) and have drawn on practice theory (e.g., Schatzki et al., 2001; Feldman & Orlikowski, 2011). For information security research, the call is thus for studies that deepen our understanding and capture in detail the social and material processes which are associated with the journey of InfoSec policy crafting.

To conclude the above discussion, the main motivation for and the research gap addressed in this dissertation is that while InfoSec policies are crucial for organizations and the policies are seldom translated into organizational practice and complied with, scholarly understanding of how InfoSec policies are accomplished in practice and how this practical accomplishment is implicated in policy compliance has yet to emerge. Practitioners are left with a map without the necessary understanding of the terrain with all its peculiarities and changing conditions.

1.2 Purpose, research questions, and delimitations

The purpose of this study is *to increase our understanding of the crafting of organizational information security policies*. To achieve this purpose, I address the following research questions:

- **Research question 1 (RQ1):** How can the challenges that surface during the crafting of an organizational information security policy be studied?
- **Research question 2 (RQ2):** How does an organizational information security policy emerge in the crafting of the policy?
- **Research question 3 (RQ3):** How is the crafting of an organizational information security policy implicated in policy compliance?

RQ1 lays the foundation for understanding InfoSec policy crafting. The question does not aim to determine the kinds of challenges that surface in the practice of InfoSec policy crafting, but at understanding how the challenges can be approached in scholarly research. RQ2 addresses a central issue of any policy – its contents. The contents of the InfoSec policy is what is expected to direct organizational actions in regard to information security. Therefore, understanding how the contents emerge is an integral part of understanding InfoSec policy crafting. Finally, RQ3 takes the perspective of InfoSec policy compliance. The assumption in this study is that policy compliance has its roots in InfoSec policy crafting.

The research questions set the boundaries for this study. Within these boundaries, the study is further delimited as follows. My interest in this dissertation is in enhancing the understanding of InfoSec policy crafting and the related phenomenon of InfoSec policy compliance as phenomena in the world; as something that happens. Therefore, this study is not about defining the crafting as a concept. Further, the study is not immediately concerned with solving practical problems or at giving advice or at providing a to-do list for InfoSec policy formulation. Indeed, information security research is not "about the solving of concrete problems by introducing yet another method and tool" (Siponen, 2005a, p. 313). Such advice would over-simplify the phenomenon and would not adequately take into account the situational and contextual aspects of policy crafting, its unfolding, and relational nature. Oftentimes, the first step is not practical problem solving, but understanding.

The study subscribes to practice-based research (cf. Gherardi, 2009), which takes "orderly social and materially mediated doing and sayings ('practices'), and their aggregations, as central to understanding organizational phenomena" (Korica et al., 2017, p. 165). Accordingly, the study focuses on InfoSec policy crafting in practice (i.e., what people do) as opposed to in theory (i.e., what people aspire to do). Further, the study is primarily about the ways in which InfoSec policy is accomplished and only somewhat about the policy itself (i.e., its contents and structure).

InfoSec policy compliance refers to a person acting in conformance with the policy. More broadly, it refers to what happens after the policy has been crafted, whether it is changes in organizational practices or people's actions, or a decoupling of the policy from organizational practices; people acting in conformance with the policy or not. The argument developed in this study is that the policy crafting process is implicated in the policy compliance. Yet, I am not concerned with measuring the compliance (as more positivist studies would do), but with practices and naturalistic experiences of those involved in the policy crafting and with the resulting policy.

1.3 Structure of the dissertation

This dissertation is structured in six chapters. The chapters and the whole dissertation are centered on five selected research publications that together form the core contribution of this dissertation. As is common for dissertations consisting of a compendium of articles, the publications were written first with their specific research foci. Although they have their specific contributions and can be understood independently from this dissertation, each of them nonetheless provides the underlying understanding and fragments that are combined together in this dissertation. Consequently, the dissertation outlines the emergent whole that arises from the publications, but more specific details and depth can be found in the publications.

Figure 1 illustrates the composition of the research publications and their relationship to the research questions. Publication IV lays the foundation for addressing RQ1 by developing a practice theory-based lens for understanding and studying the challenges of information security management in general and those of InfoSec policy crafting in particular. Publications I and II augment this understanding by further theorizing and through empirical illustrations. To address RQ2, publication I discusses how InfoSec policy emerges from information security best practices and local, situated practices through translation, and publication III discusses how policy is legitimized in the policy crafting and how this legitimization is implicated in the emerging policy. Publication V moves the discussion from the emergence of the policy contents towards policy compliance (RQ3), and illustrates how policy compliance is relational to policy crafting. It views policy compliance as the materialization of the policy in organizations' situated practices. Finally, publication II also takes a holistic view to policy crafting and touches upon each of the research questions.

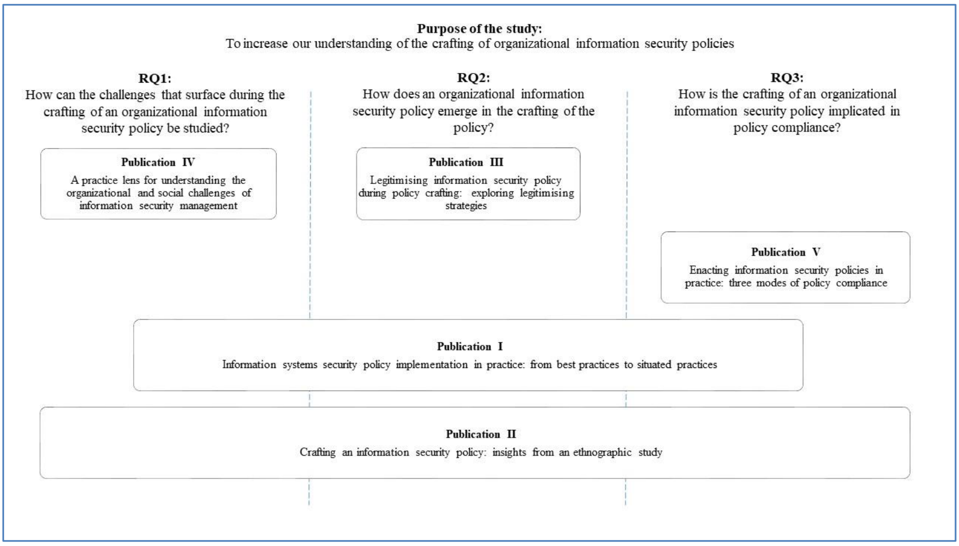
Purpose of the study:
To increase our understanding of the crafting of organizational information security policies
RQ1:
How can the challenges that surface during the crafting of an organizational information security policy be studied?
RQ2:
How does an organizational information security policy emerge in the crafting of the policy?
RQ3:
How is the crafting of an organizational information security policy implicated in policy compliance?
Publication IV
A practice lens for understanding the organizational and social challenges of information security management
Publication III
Legitimising information security policy during policy crafting: exploring legitimising strategies
Publication V
Enacting information security policies in practice: three modes of policy compliance
Publication I
Information systems security policy implementation in practice: from best practices to situated practices
Publication II
Crafting an information security policy: insights from an ethnographic study

Figure 1: Research publications and research questions

The chapters of this dissertation discuss different themes as follows. Chapter 1 introduces the study by presenting its motivation, purpose, and research questions. Chapter 2 presents the study's theoretical background by discussing the literature on information security management and InfoSec policies, and by introducing practice theory as a general sensitizing framework for this study. Chapter 2 concludes by integrating the literature on InfoSec policies and practice theory to outline their meaning towards understanding InfoSec policy crafting. Chapter 3 details the study's qualitative research approach. It briefly presents two ethnographic studies, and one case study included in this dissertation along with the construction of the empirical material and analysis. Chapter 4 presents the findings of the study by summarizing the research publications included in this dissertation and by addressing each of the research questions. Chapter 5 integrates the findings into an emergent whole and discusses their implications for research and practice. Chapter 6 briefly concludes the dissertation by suggesting its primary contributions. It further discusses the study's limitations, proposes some avenues for future research, and evaluates the study's quality.

2 THEORETICAL BACKGROUND: FROM ORGANIZATIONAL INFORMATION SECURITY POLICIES TO INFORMATION SECURITY POLICY CRAFTING

In this chapter, I outline and elaborate the theoretical background from which this study draws its foundation. The theoretical background builds broadly upon two previously isolated research streams: information security management and practice theory (see Figure 2).

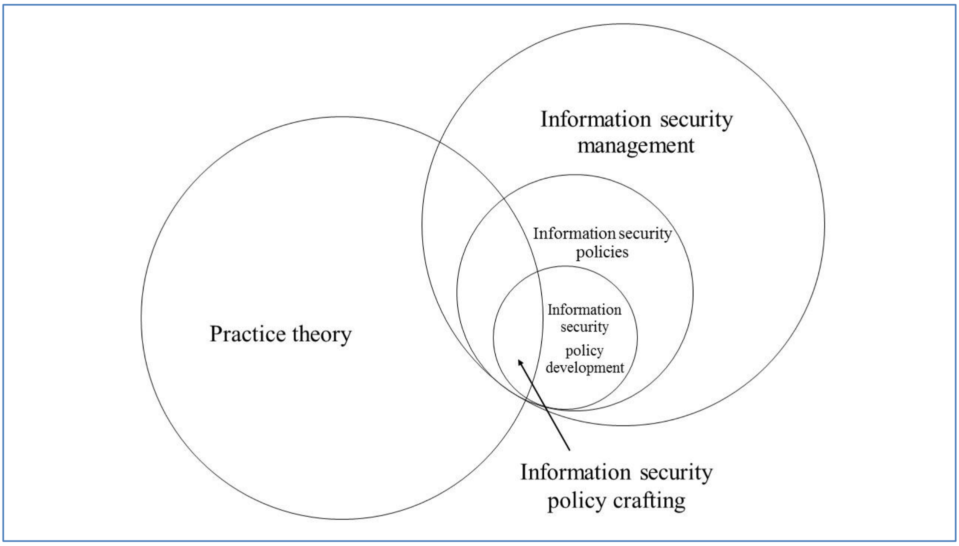
Information security management
Information security policies
Information security policy development
Practice theory
Information security policy crafting

Figure 2: Focus of the study

The chapter is structured as follows. First, I briefly introduce information security management literature in order to establish the crafting of the organizational information security policy (InfoSec policy) as a central activity of information security management. Second, I turn to the literature on InfoSec policies and discuss their importance to and role in securing organizations' information assets, their structure and content, and compliance to policies. Third, I lay down the current understanding of InfoSec policy development. Fourth, I describe the practice theory perspective as a general sensitizing framework for this study and its implications for the study. Finally, I integrate the literature on InfoSec policies and practice theory to outline their meaning towards understanding InfoSec policy crafting. Figure 2 illustrates the research streams discussed in this chapter and how InfoSec policy crafting can be situated among them.

2.1 Information security management

Information security refers to preserving the confidentiality, integrity, and availability of information (ISO/IEC, 2014). The concept of "information security" varies in meaning depending on the context of its use and from the view point taken. It can refer to technical issues (e.g., network security, firewalls, cryptography) or more managerial and organizational issues (e.g., governance structures, policies, processes, or employee behavior). In organizations, information security incorporates technology, processes, and people (Straub & Welke, 1998; Dhillon & Torkzadeh, 2006). In other words, information security is not only about technical measures but has significant social and organizational dimensions (Dhillon & Torkzadeh, 2006).

While information security research has traditionally been dominated by mathematical sciences and by a technical context, centering around issues of access to information systems (IS) and secure communication (Siponen & Oinas-Kukkonen, 2007), more recently, researchers and practitioners alike have argued that such an emphasis has significant limitations. For example, Straub et al. (2008) argue "the likely problem today is not the lack of technology, but its intelligent application" (p. 5). In the same vein, Hsu et al. (2012) suggest that "overall, information security is still in the primitive stages in terms of the management of information security rather than in terms of the extensiveness of security technologies adopted by organizations" (p. 920).

To respond to these concerns, literature on information security management is emerging. This literature is concerned with how organizations should manage and how they actually manage activities aimed at preserving the confidentiality, integrity, and availability of the organization's information. In the literature, information security management is often presented as a process or a framework for planning, implementing, and monitoring an organization's information security controls (i.e., technical, operational, and management measures aimed at preserving the confidentiality, integrity, and availability of an organization's information), and through the characteristics of that process or framework. More broadly, the focus of information security management is in "managerial actions that promote a secure environment" (Ransbotham & Mitra, 2009, p. 122).

Several information security management frameworks have been developed by both researchers and practitioners. Most of them posit information security management as a process. For example, Björck (2005) describes information security management as a process that includes the three phases of:

1. *Evaluation*, during which the current state of an organization's information security is assessed, and that results in reports of vulnerabilities and deficiencies in regard to the organization's information security;
2. *Formation*, during which controls to find vulnerabilities and deficiencies are designed and developed; and
3. *Implementation*, where the selected controls are implemented.

In addition to these phases, a feedback-operation provides information about the implemented controls for information security managers to evaluate the performance of the controls.

Straub and Welke (1998), in turn, emphasize the formalized planning and feedback mechanisms in their process and propose the five phases of:

1. *Recognition of the security problem or need*, during which problems related to the risk of information security breaches are identified;
2. *Risk analysis*, during which information security risks inherent in the identified problem areas are analyzed;
3. *Generation of control alternatives*, during which solutions to the analyzed risks are generated;
4. *Decisions*, during which information security projects are selected and prioritized; and
5. *Implementation*, during which the planned information security controls are implemented into the on-going information security of the organization.

In addition to frameworks developed by scholars, some researchers suggest that information security management should draw on "best practices" outlined in international information security management standards such as ISO/IEC27001, or maturity models such as the system security engineering capability maturity model (SSE-CMM; e.g., Von Solms, 1999; Saint-Germain, 2005; von Solms, 2005; Ma et al., 2008). Such standards and models also depict information security management as a process. For example, ISO/IEC (2013a) underlines that information security management should be a continuous, formalized process of identifying, selecting, implementing, and monitoring information security controls.

In contrast to proposing a framework, some researchers propose characteristics of an information security management process or list issues the process should cover. Trcek (2003) argues that information security management requires an integrated approach that links together technology, organizational issues, and legislation; by drawing on both practitioner and research literature, he provides a list of what information security management should attend to, such as threats analysis and risk management, security infrastructure, technological compliance, systems analysis, and design as well as information security policy. Similarly, Trompeter and Eloff (2001) propose a list of issues an organization's information security management should include such as information security policies, baseline standards, adherence to the law, and information security awareness. In the view of Eloff and Eloff (2005), a successful information security management approach should be holistic, encompassing, and measurable as well as comprehensive in regard to information security risk management. It should further suggest a predetermined set of phases to be followed and how different controls are integrated into the organization.

Common to the proposed frameworks and the proposed characteristics, as well as international information security management standards and "best practice" guidelines, is the argument that an organization's InfoSec policy lays the foundation for the information security management process. Therefore, I will next discuss InfoSec policies.

2.1.1 Information security policies

The concept of InfoSec policy is central to information security management literature. An InfoSec policy is a direction-giving document for information security within an organization (Höne & Eloff, 2002b) that communicates the organization's posture in protecting its information. Its objective is to "provide management direction and support for information security in accordance with business requirements and relevant laws and regulations" (ISO/IEC, 2013a, p. 10). It either includes both the information security objectives of an organization and the designated means and methods to achieve those objectives (Karyda et al., 2005), or the means and methods may be included in the lower-level policies (Baskerville & Siponen, 2002). Typically, the InfoSec policy further highlights the roles, rights, and responsibilities related to information security management (Hong et al., 2006; Whitman, 2004).

Researchers and practitioners alike agree that the InfoSec policy plays a central role in an organization's information security management, and advocate the InfoSec policy as laying the foundation for an organization's information security (e.g., Baskerville & Siponen, 2002; Siponen & Iivari, 2006; Warkentin & Johnston, 2008; Doherty et al., 2009). Researchers have argued that the InfoSec policy is one of the most important information security controls (Höne & Eloff, 2002a) and a prerequisite for effective information security management (Fulford & Doherty, 2003) in an organizational context. Indeed, a strong consensus exists within the extant literature that the InfoSec policy is the key mechanism for promoting effective information security management practices (Doherty et al., 2009; Herath & Rao, 2009), even to the extent that Dhillon (2007) argues: “It goes without saying that a proper security policy needs to be in place” (p. 105).

Despite its acknowledged importance, a literature review found that only 1.64% of 1,280 articles surveyed could be categorized under the topic, “security policies” (Siponen et al., 2008). Furthermore, in another literature review on information security contributions, Siponen and Oinas-Kukkonen (2007) found that the literature has a technical bias with respect to InfoSec policies. According to their review, the research on InfoSec policies has focused on “small-scale formal policies, rather than higher level and/or organizational security policies” (p. 72). The formal policies refer to the different technical rules applied to IS. Nevertheless, given the perceived importance and the centrality of the InfoSec policies for organizational information security management, it is not surprising that researchers have examined them from a variety of angles such as structure and content, as well as investigated compliance and non-compliance to the policies. Next, I will discuss these topics.

InfoSec policy structure. Information security documentation can assume different structures; usually, the documentation consists of a hierarchical set of policies and supplementing guidelines and instructions. Some researchers have discussed whether there should be a single InfoSec policy or if it should be subdivided into several different levels of documents. For example, Baskerville and Siponen (2002) suggest a three-level policy hierarchy:

1. *A high-level, organizational InfoSec policy* that embraces the general information security goals and acceptable procedures of an organization;
2. *Lower level policies* that define the selected information security methods and that guide the present and future information security decisions; and
3. *A meta-policy* that defines how an organization creates and maintains its InfoSec policies. In practice, a meta-policy defines who is responsible for formulating the policies, when they are formulated, and how they are formulated.

In contrast, Warkentin and Johnston (2008) use the terms (1) policy, (2) procedure, and (3) practice. In their terminology, policy can be either formal or informal and is formulated in order to achieve “missions and goals” (p. 47). Procedure refers to information security procedures and standards that are explicit and structured, and include formalized and specific steps for people and processes to follow. Practice, then, refers to the operationalization of the policy through execution of the procedures. Similarly, hierarchical delineation of the InfoSec policy is reflected in other studies as well (e.g., Palmer et al., 2001; Whitman, 2008). In addition to these conceptual studies, an empirical study among universities found that most universities in the sample (n = 122) had an InfoSec policy accompanied by a set of other policies, such as an acceptable use policy and an electronic mail policy, and it was supplemented by a number of specific guidelines and/or practice-related documents (Doherty et al., 2009).

InfoSec policy content. In addition to the literature on the InfoSec policy structure, the content of the policy has received attention in the academic discussion. Some researchers argue that InfoSec policy content can be directly derived from international information security management standards (e.g., Höne & Eloff, 2002b) and should include:

- The need for and the scope of information security in an organization
- Organization's objectives for information security
- Organization's definition for information security
- Organization's management's commitment to information security
- Roles and responsibilities related to information security
- Issues related to the policy itself, such as the purpose of the policy and approval, monitoring and review of the policy

De facto information security management standard ISO/IEC 27001 (ISO/IEC, 2013a), indeed, provides advice on the kinds of issues the policy should address. These include information security objectives or a framework for setting such objectives, and a statement of commitment to satisfy relevant requirements related to information security and to continually improve an organization's information security management system. However, the advice that such standards postulate have been subject to limited academic scrutiny (Doherty et al., 2009).

A more theory-driven approach to InfoSec policy content is taken in a conceptual paper by Siponen and Iivari (2006). Using a design theory approach, they propose six design theories (see Walls et al., 1992, in Siponen & Iivari, 2006) for policy content based on normative theories developed in philosophy. In line with the design theory approach, InfoSec policy is viewed as a design product, and policy formulation as a design process consisting of a set of phases to be followed. The product further includes application principles that define how the policy should be applied. The proposed principles vary according to the theory they reflect. For example, the application principle for conservative deontological design theory states "follow the list of do's and don'ts literally" (p. 456), and for liberal-intuitive design theory "[w]hat is not explicitly denied is allowed" (p. 457). Siponen and Iivari (2006) further argue that a different design theory applies to organizations in stable business environments and those having a rule-oriented culture (i.e., employees who act by the book), and to those operating in turbulent environments. Such differences affect how comprehensive the policy content should be and how exceptions to policy should be addressed.

Rather than generally prescribing what the InfoSec policy should contain, Fulford and Doherty (2003) and Doherty et al. (2009) have explored the contents of authentic InfoSec policies empirically. Doherty et al. (2009) analyzed InfoSec policies from top-ranked universities (122 universities of which 61 had an InfoSec policy available on their internet site), and found that the most extensively covered issues were violations and breaches of information security, user access management, contingency planning, and physical security. Employee responsibilities in regard to information security were also covered by most (67%) policies. Still, the scope of the issues covered in the university policies was rather limited and reflected a highly techno-centric view of information security management.

A different view to InfoSec policy content is provided by another empirical study that reviewed InfoSec policies through a critical theoretical lens by applying a critical discourse analysis (Stahl et al., 2012). This analysis showed that InfoSec policies can have a role and purpose that are rather different from what is usually advocated; ideology as a shared, but one-sided view of reality pervaded InfoSec policies. The policies further contained hints of creating legitimacy to reproduce and uphold ideology through hegemonic practices, such as quoting laws and regulations and suggesting, or directly stating that employees are subject to surveillance and possible sanctions.

In addition to the content of the InfoSec policy, how the content is presented in the policy has been suggested to affect its impact an on organization's information security. The comprehensiveness of the content has been argued as a prerequisite for an effective InfoSec policy (Hong et al., 2006). Further, breadth, clarity, and brevity have been used to characterize how well an InfoSec policy is written (Goel & Chengalur-Smith, 2010). Breadth refers to how comprehensive the policy is. Clarity has connotations of ease of understanding and reading the text included in it. Brevity refers to how compactly the information is presented; wordiness, repetitiveness, and verbose language may lead to confusion among readers of the policy and, therefore, to a less "effective" InfoSec policy. A more specific quality criteria for the InfoSec policy content emphasizes that the content should be well adapted to organization's current work practices (Karlsson et al., 2017).

InfoSec policy compliance. The structure and content of the InfoSec policy are its "architectural factors" (Whitman, 2008) that may help organizations achieve the outcomes they expect from the InfoSec policies. Although some organizations may engage in policy-practice decoupling – adopt a policy but not actually implement it (Bromley & Powell, 2012), typically, the expected outcome is that the policy is translated into actions (Warkentin & Johnston, 2008). Yet, in practice, there is often a conflict in the espoused theory and the theory-in-use, that is, what is mandated by the policy is not translated into practice (Dhillon, 2007, p. 116). Accordingly, one of the most visible developments in information security management studies is the increased interest in InfoSec policy compliance. These studies analyze how the policy can be turned into actions after it has been developed.

Compliance to an InfoSec policy refers to a person acting in conformance with the policy. Several studies contend that employees' failure to comply with the organization's InfoSec policy is a major concern for organizations. Researchers have investigated various antecedents of policy compliance and non-compliance using theoretical foundations from, for example, organizational behavior, the technology acceptance model (TAM), and social influence (Warkentin & Willison, 2009). Such studies investigate employees' intentions to comply with the InfoSec policies (e.g., Herath & Rao, 2009; Siponen et al., 2010; Warkentin et al., 2011; Vance et al., 2012; Johnston et al., 2015), or provide insight into the causes of non-compliance (e.g., Myyry et al., 2009; Johnston et al., 2016), or develop a method for analyzing different rationalities behind employees' compliance and non-compliance (Kolkowska et al., 2017). Findings from such studies have advanced our understanding of the insider motivations and psychological factors that relate to InfoSec policy compliance and non-compliance. Although the authors suggest that their findings should be incorporated in InfoSec policy development, listing insider motivations or psychological factors tell little about how they could be incorporated in an organization's InfoSec policy. Thus, the focus of the next section is whether situated actions must take place when InfoSec policy is developed in order to be incorporated.

2.1.2 Information security policy development

Since the purpose of this study is to increase our understanding of the crafting of InfoSec policies, I now turn my attention to the activities that define this work. In contrast to the research described in Section 2.1.1, "Information security policies," which is largely concerned with what policy "is," the research on InfoSec policy development is interested in how to "accomplish" a policy.

Information security management standards. Traditionally, information security management standards and "best practice" guidelines, such as international ISO/IEC27001 (ISO/IEC, 2013a) and ISO/IEC27002 (ISO/IEC, 2013b) standards and the American National Institute of Standards and Technology (NIST, 2006) standard family, have played a central role in information security management (for empirical studies, see Backhouse et al., 2006; Smith et al., 2010; Hsu, 2009). Information security best practices are documented descriptions that have been collected from different organizations through standardization processes (Backhouse et al., 2006), and which aim to define what organizations should do in regard to information security. They generally require that an organization must establish an InfoSec policy.

Organizations increasingly face institutional pressure to adopt the best practices to their policies (Hsu et al., 2012). However, the best practices do not address how policy could or should be accomplished in practice (Siponen, 2006). Instead, they merely provide suggested definitions and characteristics of the policies. For example, the ISO/IEC27001 standard requires organizations to establish an InfoSec policy (i.e., clauses 5.1 and 5.2), but does not address how this could be achieved. The accompanying implementation guide, ISO/IEC27002, is no more informative as it only describes what issues the policy should address. The fact that neither standards nor best practice guidelines address InfoSec policy development is one motivation for studies on InfoSec policy development.

InfoSec policy development methods. In the literature, development of an InfoSec policy is commonly depicted as a series of discrete phases. Both empirical and conceptual studies exist that suggest a set of phases for policy development (see Table 2 for recent contributions). The methods are general and abstract in the sense that it is easy to see that on a high level they could characterize any InfoSec policy development.

In a conceptual paper, Whitman (2008) suggests five phases for InfoSec policy development: (1) investigation; (2) analysis; (3) design; (4) implementation; and (5) maintenance and change. The investigation phase addresses the question of "what is the problem the policy is being developed to address" by examining the event or a plan that initiated the policy development process and specifies the objectives, constraints, and scope of the policy. The following analysis phase consists of an assessment of the organization, its current policies, and the anticipated perceptions of those who will be affected by the new policy. The design phase uses the information from the analysis phase to formulate a policy draft, which is provided for relevant parties to review and comment. After the design phase, policy implementation and finally policy maintenance and change commence.

In another conceptual paper, Rees et al. (2003) propose a policy development method they coin: "A Policy Framework for Interpreting Risk in E-Business Security" (PFIRES). It consists of four major phases: (1) assess; (2) plan; (3) deliver; and (4) operate. Each phase includes two discrete steps which are again divided into sub-steps executed in a sequence. The phases and the steps are described in some detail, but the description is on the level of what should be done, and not how it could or should be done. The process acknowledges that InfoSec policy development is an iterative process, and therefore includes feedback loops for each phase.

Knapp et al. (2009) propose a model of the InfoSec policy development method based on the results of a survey. The resulting model views InfoSec policy development as a repeatable flow of activities that consists of eight phases: (1) risk assessment; (2) policy development; (3) policy approval; (4) policy awareness and training; (5) policy implementation; (6) monitoring; (7) policy enforcement; and (8) policy review. The model further depicts the need to execute some of the phases repeatedly by suggesting that there may be iterations within them and between them as well as iterations of the whole flow of activities. The phases themselves are not further elaborated. For example, the content of the policy development phase is left as a black box. Consequently, the model is meant to depict the phases involved in InfoSec policy development, rather than how the phases could or should be executed.

Table 2: Phases for information security policy development

	Whitman (2008)	**Knapp et al. (2009)**	**Rees et al. (2003)**	**Corpuz & Barnes (2010)**	**Flowerday & Tuyikeze (2016)**
Development	Investigation		Assess: policy assessment and risk assessment		
	Analysis	Risk assessment		Security risk assessment (develop InfoSec policy)	Risk assessment
	Design	Policy development, Policy approval	Plan: policy development and requirements definition		Policy construction
Implementation	Implementation	Policy awareness and training, Policy implementation	Deliver: controls definition and controls implementation	Security risk treatment (implement InfoSec policy) Security risk acceptance and communication (communicate InfoSec policy)	Policy implementation
Monitoring	Maintenance and change	Monitoring, Policy enforcement, Policy review	Operate: monitor operations, review trends, and manage events	Security risk review and monitoring (review and monitor InfoSec policy)	Policy compliance, Policy monitoring

Other methods for InfoSec policy development have been suggested, such as aligning InfoSec policy development with corporate risk management (Corpuz & Barnes, 2010) or with an organization's strategic IS plan (Doherty & Fulford, 2006). The methods provide varying levels of detail, but the suggested major phases are largely similar: development, implementation, and monitoring (see Table 2). Development is about defining the structure and content for the policy; implementation is about different means for translating the policy into actions; and monitoring is about overseeing the policy's influence on the organization and making changes to the policy when needed.

The purpose of the policy development methods seems to be to establish phases through which policy development should flow. Thus, the research efforts have not been so much directed towards the actual development of the policies, but towards methods and models of their production. As research has focused on the methods and has sought to abstract universal phases for developing policies, it has tended to assume that actual policy development practices follow rather directly from such methods. Yet, there is evidence that the process is not a set of phases but an emergent one (Dhillon, 2007, p. 126). Policy development should, therefore, be analyzed from the perspectives of the people involved (Dhillon, 2007, p. 126).

Actors involved in InfoSec policy development. Different actors – not only information security professionals – within an organization should participate in information security management activities. Employees' (or users') participation in information security management activities, such as information security risk management, may improve their perception about the significance of information security measures (Spears & Barki, 2010) and may promote social acceptance of security techniques and procedures (Siponen, 2005b). Employees' participation in InfoSec policy development has been identified as one of the critical contextual factors for a successful policy outcome (Karyda et al., 2005). In a previous study, employees further expressed their interest in participating in access control policy development (Ferreira et al., 2010).

The role of employee participation is highlighted in a qualitative, grounded theory study conducted within the healthcare sector (Adams & Blandford, 2005). The study is not about InfoSec policies per se, but about employees' involvement in organizations' information security and privacy initiatives. In the first studied hospital, information security professionals sought to negotiate with different user communities in order to agree on practices for new policies and procedures; their efforts increased users' perceived ownership of organization's information security mechanisms. The study at the second hospital, in turn, highlights that InfoSec policies developed and implemented without employee participation may increase negative perceptions of the InfoSec policies among the employees. Based on the study's results, the authors suggest that information security professionals should develop appropriate links with communities of users in order to develop appropriate procedures that users are motivated to complete, and by doing so, avoid traditional authoritarian approaches to disseminating InfoSec policies. As the aforementioned suggests, employees' participation in InfoSec policy development may be useful in achieving expected policy outcomes. Situated studies on InfoSec policy development uncover other issues policy development methods abstract away.

Developing an InfoSec policy in an organizational context. An InfoSec policy is always accomplished as situated work in a certain context; something that the aforementioned InfoSec policy development methods pay little or no attention to. In context, people are more than employees or users; they bring about the social dynamics and emergent challenges (i.e., challenges that surface in the practice of doing) to InfoSec policy development. The context further involves more than people. Using Pettigrew's theory of contextualism (Pettigrew, 1987, in Karyda et al., 2005), Karyda et al. (2005) analyze how InfoSec policy development and implementation are affected by the context and by the power relationships and cultural elements within which they happen in two case studies. The contextual analysis of the content, context, and process dimensions of the InfoSec policy development and implementation provide insight into related changes at the organizational, work system, and information technology levels and into cultural and power aspects that shape these processes.

Whereas the focus of Karyda et al. (2005) is broadly defined as the "context" of InfoSec policy development and implementation, power relationships have been the specific focus of a few empirical studies. In particular, the impact of power on InfoSec policy development and implementation has been analyzed through the theoretical lens of theory of circuits of power (Clegg, 2002, in Lapke & Dhillon, 2008). A case study conducted by Lapke and Dhillon (2008) illustrates how organizational groups without formal power (i.e., implicit power groups), such as subject matter experts, may exercise power over both InfoSec policy development and implementation. They further find that employees' resistance towards the InfoSec policy may be a result of the policy's negative effect on employees' productivity. They postulate that the resistance may cause changes to the implementation of the InfoSec policy, and that an important moderating factor to this relationship is the degree of impact the implementation has on employees' productivity.

Power relationships and their impact was also the topic of Lapke's (2008) dissertation. Using the theory of circuits of power and data from an interpretive case study, Lapke (2008) concludes that organizational power may impact InfoSec policy development in three ways. First, existing power relationships have an impact on its development, and existing and explicit power structures are reinforced by the fact that existing structures are designed to prevent end-users, the lowest end of the organizational power spectrum, from taking part in InfoSec policy development. Second, the transformation of the studied organization towards centrally managed InfoSec policies, centralized the power structure responsible for the InfoSec policy development. Third, the findings of the study suggest that traditionally disempowered employees may affect the policy development. Even though these employees hold low operational positions in the organizational hierarchy, they may have a significant informal influence on policy development through their informal power relationships.

Power relationships do not only affect policy development and implementation, but may have an impact on InfoSec policy compliance as well. Indeed, an organization's inability to understand different power dimensions (here, the dimensions suggested by Hardy, 1996, in Kolkowska & Dhillon, 2013; i.e., resource-based power, process-based power, meaning-based power, and system-based power) during InfoSec policy development and implementation may lead to non-compliance with the policy (Kolkowska & Dhillon, 2013). In a case study, the studied organization failed to realize the expected policy outcomes because the organization's management understood power only in relation to resources, and did not understand the power that resided in the organizational structures. More broadly, information security cannot be imposed by rule "as 'Hobbesian' or sovereign power, but emerges from the interplay of social and technical actors" (Inglesant & Sasse, 2011, p. 9). That is, while written InfoSec policies and endorsement by senior management are the necessary foundations of information security, those have little to say about the day-to-day enactment of the InfoSec policies in everyday organizational practices. What they mean by enactment refers to employees' daily interactions with the policies and how those influence employees' work or how those are circumvented by the employees.

In addition to power relationships, value conflicts may impact policy development in an organizational context. Hedström et al. (2011) propose that organizational actions employ multiple forms of rationality that may cause value conflicts. Such conflicts should be accounted for in InfoSec policy development.

To conclude this section, the existing research suggests different methods for developing an InfoSec policy. Characteristic of such research are contributions based on conceptual development and suggestions of methods for policy development that subscribe to something Baskerville and Dhillon (2008) would call universal cookie-cutter strategies; strategies that include an overall framework that is described in such general terms that it, with contingencies, suits any organization. Arguably, this body of research provides insights into policy development. However, as it aims at developing universal guidelines, it seems to offer descriptions of what should be done without attending to the "ground realities" and the challenges of the InfoSec policy development in practice. Yet, as Siponen (2006) argued for information security standards, the "existence of prescribed security processes in organizations does not mean the goals of the processes are achieved" (p. 97). Therefore, an emerging research stream analyzes employees' participation in policy development and studies contextual factors of policy development such as power.

2.2 Practice theory

In this study, I use practice theory as a general sensitizing framework – as "a flexible theory–methods toolkit suitable for analytically engaging situated insights, toward furthering rich, empirically based understanding" (Korica et al., 2017, p. 152). This section outlines this sensitizing framework for understanding and theorizing InfoSec policy crafting by highlighting the situated, relational, emergent, sociomaterial, and consequence-oriented analytical foci the framework suggests.

Literature reviews on information security management highlight the lack of theoretically grounded empirical studies in this area, and particularly, the social aspects of information security management methods (Siponen, 2005a, 2005b; Siponen & Oinas-Kukkonen, 2007). Hence, it is difficult for scholars to conceptualize the underlying information security management problems, which successively hinders finding practical solutions to those problems (Stahl et al., 2012). Indeed, more theoretically grounded research that uses empirical methods is needed to increase our understanding of information security management (Siponen et al., 2008). In this study, I build on these suggestions and frame my study theoretically within the emerging field of practice theory. Whereas practice theory is a broad intellectual landscape without a uniform canon, my reading and use of it draws mostly upon the version outlined by Schatzki (2001, 2002, 2005, 2006),[1] and upon the core principles of the practice theory introduced by Feldman and Orlikowski (2011). These principles can be summarized as follows:

1. Situated actions are consequential in producing social life;
2. Different dualisms between, for example, objective and subjective, structure and agency, individual and institutional, mind and body, cognition and action are rejected; and
3. Phenomena exist in relation to each other and are produced as a process of mutual constitution.

Practice theory focuses researchers' attention on developing an account of practices, and argues that the field of practices is the arena for studying organizations (Schatzki et al., 2001). The practice theory perspective and the research drawing on it are characterized by an emphasis on situated actions, attention to the mundane, micro-level aspects of work and organizing, and how they unfold in real time and over time. According to this perspective, people draw upon practices as a set of resources in their everyday life, and at the same time, reconstitute the system of shared practices (Barnes, 2001, p. 26). Accordingly, the perspective takes social life as an ongoing production that emerges through actions (Feldman & Orlikowski, 2011). In contrast to a focus on ahistorical discrete entities contingently linked in aggregates, the perspective acknowledges the irreducibly situated nature of the reality people experience (Sandberg & Tsoukas, 2011). It further pays attention to how the detailed activity and societal context are closely linked (Whittington, 2006). People are both enabled and constrained by organizational and wider social practices (Vaara & Whittington, 2012). Finally, the term "practice" signals researchers' commitment to theories of practice and their

[1] Publication V builds theoretically on the sociomaterial practice perspective as delineated by Barad (2003, 2007).

attempt to be close to the world of the practitioners (Vaara & Whittington, 2012). The value of such a perspective lies in challenging the "structure of causality assumed in many traditional models and showing how structures associated with technologies, knowledge, accounting, and so forth are not fixed but, rather, constituted by particular actors in particular circumstances" (Kaplan, 2007, p. 986).

According to Schatzki's (2001, 2002, 2005, 2006) account, social life transpires as and amid practices and something he calls material "arrangements." In general terms, practices can be conceived as "arrays of activity" that are materially mediated and organized around shared practical understandings (Schatzki, 2001). A practice forms a "block" whose existence necessarily depends on the existence and specific interconnectedness of different elements (e.g., forms of bodily and mental activities, "things" and their use, understanding), and which cannot be reduced to any one of these single elements (Reckwitz, 2002a). Hence, practices are more than "just doing," as the commonsensical definition might suggest. More precisely, any given practice is composed of actions, and these actions are organized by three phenomena: "understandings of how to do things, rules, and teleoaffective structure" (Schatzki, 2005, p. 471). Understandings refer to practical understandings about the actions constituting the practice and to general understandings that are components of practices that are tied to the site of which some practice is a part; thus, they are common to several practices of that site. Rules are explicit formulations that prescribe or instruct something to be done or said. Teleoaffective structure denotes acceptable ends, projects, uses of things, and perhaps even emotions for the actors of a given practice. Rules or ends to be pursued are not carved in stone but disagreements about them may lead to questioning a practice (Schatzki, 2002, p. 84).

Drawing on Schatzki (2005), actions that constitute information security management practices could plausibly be organized by: (1) shared understandings of, for example, how to plan, implement, and monitor information security controls, develop InfoSec policies, and obtain a budget for information security activities and general understandings of efficiency and risk mitigation; (2) those who observe, violate, or ignore the same rules, guidelines, or requirements such as contracts that govern information security management, international information security management standards and "best practice" guidelines and rules of thumb about measuring the effectiveness of certain information security controls; and (3) seek ends and projects included in the same teleoaffective structure such as preserving the confidentiality, integrity, and availability of an organization's information, and assuring necessary InfoSec policy compliance within the organization. In short, practices can be understood as meaning-making, order-producing, and identity-forming activities that imply meditational tools and a community of peers (Feldman & Orlikowski, 2011; Nicolini, 2009a).

Researchers interested in practices have come to acknowledge the importance of materiality in the "production of social life" (Feldman & Orlikowski, 2011, p. 1242). Therefore, in drawing on any practice theory perspective, one must analyze how "bundled activities interweave with ordered constellations of nonhuman entities" (Schatzki, 2001, p. 12) such as artifacts and objects. Barad (2007) explains that from a sociomaterial practice perspective (see publication V), matter and meaning are not clearly demarcated or fixed but in a flux of becoming. Materiality in part constitutes social life. Various material arrangements are likewise central to Schatzki's practice perspective. In particular, by material arrangements, Schatzki means "set-ups of material objects" (Schatzki, 2005, p. 472) that encompass people, other living organisms, artifacts, and things, and in which these entities all relate, occupy positions, and enjoy meanings (Schatzki, 2002, pp. 20–21). Any setting within which an actor acts and thereupon carries on a practice is composed of different material entities such as other actors and artifacts. It is plausible to expect that any crafting of an InfoSec policy is a bundle of practices and material arrangements.

Next, I discuss five reasons why the practice theory perspective is a relevant theoretical sensitizing framework for this study, and I outline certain implications of this perspective for this study. First, the perspective views the participating actors of a given practice not as passive but as active and intentional (Barnes, 2001, pp. 25–26). Actors do not slavishly "follow" the practices, but are their "artful interpreters" (Bourdieu 1990) and draw upon them as a "set of resources" in the course of actors' activities (Barnes, 2001, p. 26). Therefore, actors' initiatives and practical skills make a difference (Whittington, 2006) to information security management activities, and their situated actions are consequential in the production of social life in a given organization (Feldman & Orlikowski, 2011). Yet, theories of practice do not start from any individual and her/his intentionality in pursuing courses of action, but view actions as "taking place" or "happening," "as being performed through a network of connections-in-action, as life-world and dwelling" (Gherardi, 2009, p. 115). It follows that this study accounts for actors involved in InfoSec policy crafting, but focuses on their actions more than on their intentionality.

Second, not only are actors intentional, but from Schatzki's account, elements of intentionality are also inscribed in practices. Practices are oriented towards the future, towards a teleoaffective structure that includes sets of ends and projects acceptable within the practice. Thus, practices govern and organize actors' activities by inscribing acceptable ends and projects for them. Actors involved in a practice experience it as "being governed by a drive that is based on both the sense of what to do and what ought to be done" (Nicolini, 2009a, p. 1403). This is relevant for this study as several information security management practices do have a teleological orientation; clear ends or projects are inscribed into them. This is particularly true for information security best practices that prescribe certain actions or processes (Siponen, 2006). General understandings may further guide a set of such practices in a more indirect way, such as a concern for protecting the organization's information proportional to the risks for the information or a concern for efficiency. This governing capacity of practices implies that by understanding the practices that actors enact when crafting an InfoSec policy and the ends or projects inscribed in the practices, we can better understand InfoSec policy crafting.

Third, the practice perspective affords understanding how InfoSec policy crafting happens and with what kinds of emergent implications both during and after the process. It supports an investigation of "becoming" instead of what "is," leading to a more elaborate understanding rather than a descriptive study. Prior research suggests that the perspective has the potential to reveal what actually takes place as it allows researchers to explore what the actors do as opposed to what they aspire to do (Levina & Vaast, 2005; Suchman, 2007). Therefore, the perspective supports an investigation that aims to move closer to the InfoSec policy crafting in practice and allows for understanding the InfoSec policy crafting that includes situated, social, and temporally evolving aspects thus far neglected to a large extent by the dominant discourse in information security management literature. As discussed in Section 2.1.2, "Information security policy development," existing research is more concerned with the phases of InfoSec policy development than with how such development unfolds.

Fourth, the perspective may reveal how the practices enacted during InfoSec policy crafting may alter or sustain the existing information security direction in an organization. In other words, it may reveal how crafting is implicated in policy compliance. As change is inherent in human action, organizations are continuously in an ongoing process of change (Tsoukas & Chia, 2002). Even organizational routines are "emergent accomplishments" as they are performed by human actors (Feldman, 2000, p. 613). Indeed, "practice continuously changes, expands, and evolves" (Nicolini, 2009a, p. 1405). Consequently, it is plausible to expect that as InfoSec policy is crafted over time through actions of different actors, each action contains potential for either change or stability in the direction of the organization's information security management. Furthermore, according to the practice perspective, change may result from emergence and surprise; it is not necessarily the change that was initially planned or imagined.

A final, yet important, implication is related to situated actions. Whereas the extant research on InfoSec policy development has proposed abstract phases and methods for developing the policy without attending to the actual situation where such development takes place, the practice perspective results in a different emphasis. This can be understood by the perspective's emphasis on situated action. Suchman (2007) discusses the differences between what she calls a planning model and situated actions. The planning model assumes that before any action is taken, the actors involved carefully develop a plan to achieve a given end and then the actual action is a simple, effortless execution of the plan. All effort is therefore placed on planning. However, as Suchman (2007) argues, situated action is not simply an execution of a plan. Indeed, no plan can ever truly comprehensively anticipate the actual circumstances of actions, and unanticipated conditions require further planning. She goes further to suggest that developing a plan is a form of situated action. The implication is that "plans are best viewed as a weak resource for what is primarily ad hoc activity" (Suchman, 2007, p. 27). Seen from this point of view, the phases and methods suggested by scholars are necessarily vague and leave out the particularity of details of the situated action. At the same time, they leave out how actors could use the resources of a particular situation. Consequently, situated actions of the InfoSec policy crafting are central to this study.

In sum, the practice theory perspective forms the sensitizing framework of this study. Practice theory, and its different variants, were used differently and more and less explicitly in the publications constituting this dissertation. Yet, in all publications, practice theory supported investigations into the actual accomplishment of an InfoSec policy. This resulted in the analytical focus on how policy is crafted rather than what the policy's structure or content are or what kind of high-level phases its development should involve. In all publications, practices as "arrays of activity" related to the InfoSec policy crafting were the locus of the study. The sensitizing framework is further used in explaining the implications of this study in Chapter 5, "Discussion."

2.3 Synthesis

In Sections 2.1 and 2.2, I discussed information security management, InfoSec policies, and practice theory. Next, I will summarize and integrate these discussions, and elaborate on how these conceptual building blocks can help to understand InfoSec policy crafting. Specifically, I argue that much can be gained when contemporary notions of practice are brought into the study of InfoSec policies.

The literature on InfoSec policies is largely concerned with the features of the policy document, namely its structure and content, and with exploring the essential issue of translating policy into actions through analyzing reasons for employees' compliance or non-compliance to the organization's policy. Literature that is explicitly concerned with InfoSec policy development is often about policy development methods described as a series of abstract phases. Although generic abstractions such as policy development phases are certainly indispensable in guiding organizations in their efforts to develop the policy, they largely assume that the actual practices of policy development will automatically follow as soon as appropriate and accurate abstractions have been grasped. That is, developing an InfoSec policy is implicitly conceived as rather a rote procedure that follows specified steps.

The practice theory perspective argues for the opposite: situated practice is never a rote following of abstractions (Suchman, 2007). The perspective further generally argues that macro level phenomena, such as universal guidelines for InfoSec policy development, emanate from the level of practices (Schatzki, 2005). Yet, situated practices always contain parts that are invisible and can never be rendered fully visible, and which are lost when standardizing and documenting those practices (Almklov & Antonsen, 2014). Consequently, taking a practice theory perspective challenges the prevailing focus on InfoSec policy literature (e.g., InfoSec policy development methods), and advocates a more situated, emergent, and relational focus. It suggests approaching InfoSec policy development from the actual accomplishment of the policy crafting, and thus holds the promise of increasing our understanding of what the policy development phases entail in practice.

The situated, emergent, and relational focus resonates well and extends the existing research that is interested in InfoSec policy development in particular contexts (see Section 2.1.2). This emerging research suggests that InfoSec policy development is unlikely the following of a rote procedure, but involves a number of challenges. While the existing research has suggested that power relationships and the organizational context are central in understanding the challenges of InfoSec policy crafting, the practice theory perspective advocates practices as the site of the challenges and begins to build theorizations from there.

Although challenges involved in policy crafting are likely central for understanding InfoSec policy crafting, another central issue is how policy emerges in the crafting. While the existing literature suggests the kind of content the policy may include, listing the content from ready-made policies tells little about how that content emerged. The practice theory perspective is, in turn, interested in how policy crafting achieves its effects practically and in situ. Accordingly, empirical attention is not only paid to the "what" of policies or policy crafting but also to the "how" of policy crafting. The practice theory perspective provides the analytical tools for moving closer to the emergence of policy content, because it supports an investigation of what actually takes place rather than what is aspired to take place.

A central concern related to InfoSec policies is that they only seldom translate into actions. Studies on policy compliance and non-compliance seek to find ways to promote compliance to policies by investigating antecedents of policy compliant and non-compliant behavior. Accordingly, employees' intentions in pursuing courses of action are at the center of these studies. The studies further analyze the compliance and non-compliance after the policy has been developed, thus separating policy development from compliance. Instead of focusing on intentions, “theories of practice view actions as ‘taking place’ or ‘happening’, as being performed” (Gherardi, 2009, p. 115). Thus, the practice perspective can assist in understanding policy compliance as relational and situated practical accomplishment. In this study, compliance is particularly analyzed in relation to the policy crafting.

In sum, integrating the practice theory perspective into research on InfoSec policies results in an interest in how policy crafting achieves its effects practically and in situ in the flow of organizational practices. Accordingly, an analysis of InfoSec policy crafting in practice will deepen and widen our understanding of the challenges of InfoSec policy crafting, the emergence of policy content, and the implications of policy crafting to policy compliance. Figure 3 summarizes the understanding that emerges from the existing literature and situates InfoSec policy crafting among the InfoSec policy development literature (i.e., the gray area in Figure 3).

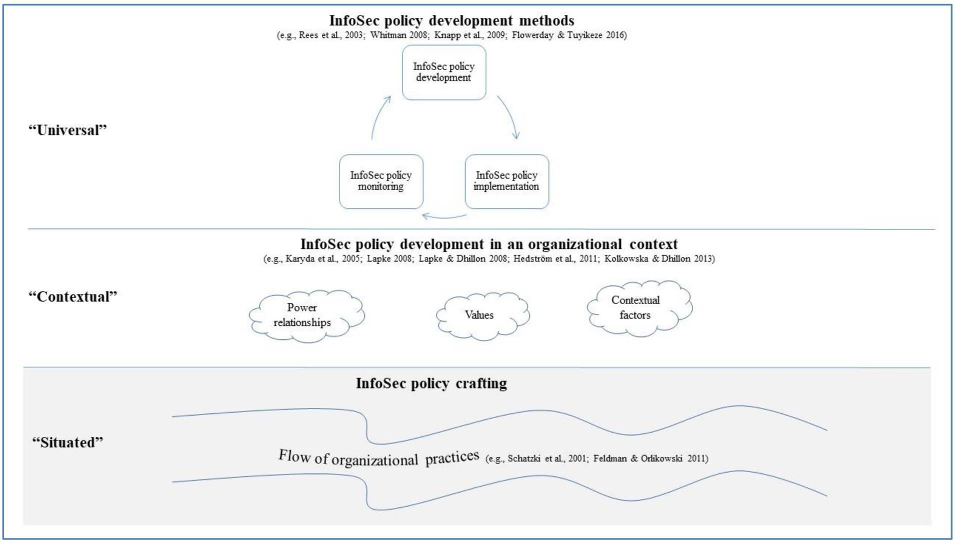
InfoSec policy development methods
(e.g., Rees et al., 2003; Whitman 2008; Knapp et al., 2009; Flowerday & Tuyikeze 2016)
InfoSec policy development
InfoSec policy implementation
InfoSec policy monitoring
“Universal”
InfoSec policy development in an organizational context
(e.g., Karyda et al., 2005; Lapke 2008; Lapke & Dhillon 2008; Hedström et al., 2011; Kolkowska & Dhillon 2013)
“Contextual”
Power relationships
Values
Contextual factors
InfoSec policy crafting
“Situated”
Flow of organizational practices (e.g., Schatzki et al., 2001; Feldman & Orlikowski 2011)

Figure 3: Information security policy development literature

3 RESEARCH APPROACH

In this chapter, I explain and reflect on the research approach of this study and its justification, given the ontological and epistemological assumptions underlying it. This study subscribes to the qualitative research tradition, and in particular, to ethnographic and case study research approaches. The study is both multi-method and multi-sited. Figure 4 illustrates the relationships between the publications and the empirical material.

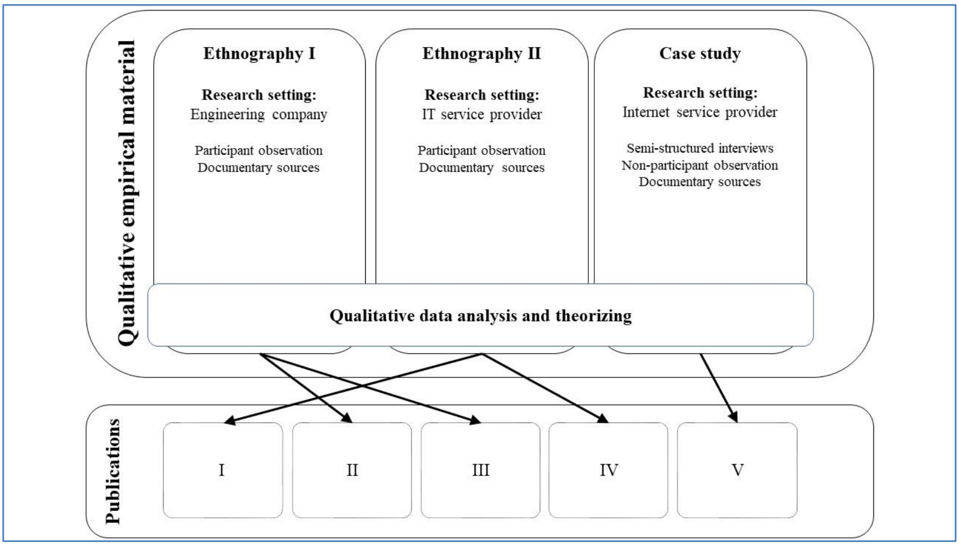

Figure 4: Publications and empirical material

The chapter is structured as follows. First, I will briefly discuss the study's philosophical basis. Second, I will outline its qualitative, ethnographic, and case study approaches. Third, I will give a short description of the research settings and my role in each setting. Fourth, I will turn to the empirical material and discuss how the empirical material was constructed through participant and non-participant observation, semi-structured interviews, and documentary sources. Finally, I will briefly illustrate the analysis of the empirical material.

3.1 Some philosophical considerations

Ontological beliefs concern the essence of the phenomenon under investigation; that is, whether the physical and social worlds are assumed to be objective and exist independently of humans, or subjective and exist only through human actions that create and recreate them. Studies that are interested in practices and that utilize some form of a practice theory may take an ontological stance that social reality is fundamentally constituted by practices (Feldman & Orlikowski, 2011). That is, rather than seeing the social world as socially constructed by human agents or as external to them, the social world is seen as brought into being through mundane activities. For example, according to Schatzki, social life transpires as and amid practices and material "arrangements" (i.e., "set-ups of material objects"; Schatzki, 2005, p. 472) that encompass people, other living organisms, artifacts, and things, and in which these entities all relate, occupy positions, and enjoy meanings (Schatzki, 2002, pp. 20–21). The social world is not "given" but continuously produced and reproduced by situated actions. Yet, the production and reproduction happens in relation to other phenomena, and phenomena are produced as a process of mutual constitution. Consequently, studies that subscribe to practice-based approaches take micro-level activities and socially legitimized sayings and doings (i.e., "practices" or modes of practicing) as their unit of analysis (Korica et al., 2017).

Practices are the arena for studying organizations (e.g., Orlikowski, 2000; Schatzki, 2001). They are seen as more than "just doing"; they are "arrays of activity" that are materially mediated and organized around shared practical understandings (Schatzki, 2001, p. 11). Practices are, therefore, order-producing, meaning-making, and identity-forming activities that are situated in particular historical conditions and that imply a plethora of material "tools" (Feldman & Orlikowski, 2011). While such an ontological view justifies the study's focus on practices, the focus "on everyday activity is critical because practices are understood to be the primary building blocks of social reality" (Feldman & Orlikowski, 2011, p. 1241); this ontology may be more or less explicit in researchers' application of practice theory. Similarly, in this study, the practice ontology is more explicit in some of the publications included in this dissertation and less in others, depending on the focus of the publication.

Epistemological assumptions concern the criteria for constructing and evaluating knowledge. Traditionally, three epistemologies have underlined IS studies of which information security management literature is a part: positivist, interpretive, and critical (e.g., Orlikowski & Baroudi, 1991). The conception of practice as epistemology constitutes a different approach. According to Gherardi (2009), practice as epistemology can be understood by the difference between theories of action and theories of practice: "While theories of action start from individuals and from their intentionality in pursuing courses of action, theories of practice view actions as ‘taking place’ or ‘happening’, as being performed through a network of connections-in-action, as life-world and dwelling” (p. 115). This means that “practice as epistemology articulates knowledge in and about organizing as practical accomplishment, rather than as a transcendental account of a decontextualized reality done by a genderless and disembodied researcher” (Gherardi, 2009, p. 124). Such a view has implications for studying the phenomenon of interest. In particular, the view implies an orientation towards understanding situated actions, attention to the mundane, micro-level aspects of work and organizing, and how they unfold in real time and over time. It further means analyzing how “bundled activities interweave with ordered constellations of nonhuman entities” (Schatzki, 2001, p. 12) such as artifacts and objects. It necessitates convincing accounts not only about the activity but also about its conditions of possibility in the amalgam of further practices (Korica et al., 2017).

Focusing on practice in the study of InfoSec policy crafting necessitates departing from certain kinds of research methods upon which information security management literature has largely been built (for an analysis of research approaches used, see Siponen, 2005a), particularly from quantification and a priori categories with the aim of producing “law-like” predictions, and is consequential for configuring processes of inquiry. First, it necessitates a focus on situated activities as they are seen as consequential in the production of social life (Feldman & Orlikowski, 2011). This means analyzing practices as they are accomplished at particular places and times and in a given historical and material context. It further means a focus on the specific instead of generalizable accounts (Korica et al., 2017). To empirically study practice, therefore, requires methods that enable observing and capturing in situ activity as it happens, and that enable making the historical and material context analytically present in the unfolding of practice. Second, it requires acknowledging that phenomena exist in relation to each other and are produced as a process of mutual constitution (Feldman & Orlikowski, 2011). Concretely speaking, this means that researchers’ focus is not on ahistorical discrete entities contingently linked in aggregates, but on “how practitioners are ordinarily involved in the *relational whole* within which they carry out their tasks” (Sandberg & Tsoukas, 2011, p. 346, emphasis in the original). Epistemologically, this calls for “strong” engagement: rich qualitative studies capable of explaining organizational actions, “instead of simply registering them” (Nicolini, 2012 p. 13). In this study, rich qualitative studies materialize as two ethnographic studies and one case study.

When the subject of the study is practice or practices, researchers can take an epistemic position of “inquiry from outside” or of “inquiry from inside,” and the position yields to different research methods. Analyzing practices “from outside” entails a focus on the recursiveness of practices, on more or less shared understandings that allow their repetition and on the patterns that organize these activities (Gherardi, 2009). In the context of an InfoSec policy, such an analysis would seek to understand the recursiveness of some activity through which the policy emerges. The focus adopted in this study, analyzing practices "from inside" or "from within" practices, has a different focus. It analyzes practices as they are being performed and takes particular account of their temporality and processuality as well as "the emergent and negotiated order of the action being done" (Gherardi, 2009, p. 117). It "zooms in" to real-time practicing as a skilled accomplishment (Nicolini, 2009a). Thus, the position of "inquiry from inside" taken in this study means a focus on the doings and what is done in the crafting of an InfoSec policy. Practices are analyzed in real-time as they are carried out in the workplace, and attention is paid to the relationships and connections among the resources and constraints present. Such a position calls for a qualitative research approach, and ethnographic and case study methods that are sensitive to the factual, material, and temporal nature of practices (Nicolini, 2009a).

3.2 Qualitative research

As the purpose of this study is to increase our understanding of a complex, largely social, phenomenon, and given the aforementioned epistemology discussion that calls for situatedness, relationality, and strong engagement, the overall research approach of this study is qualitative. The qualitative approach is further justified as the context, practices, and actions are central for this study (Guba & Lincoln, 1994). Qualitative research is a legitimate research approach in IS studies (Sarker et al., 2013), and it is in line with the previous studies that have focused on practices (e.g., Smets et al., 2012; Jarzabkowski et al., 2012). More specifically, I used ethnographic and case study approaches in the construction of the empirical material of this study; ethnographic approach was used for the publications I-IV and case study approach for the publication V (see Figure 4). Combining both approaches to one dissertation affords capturing a more complete and holistic portrayal of the phenomenon under study (Jick, 1979).

3.2.1 An ethnographic approach

Publications I and IV are based on an ethnographic study of crafting and implementing an InfoSec policy at Alpha (a pseudonym), an IT service provider. Publications II and III, in turn, are based on an ethnographic study of crafting an InfoSec policy at Beta (a pseudonym), a globally operating engineering corporation (see Figure 4). Ethnographic research is one of the most in-depth research approaches available and characterized by the researcher spending extended periods of time at the research site observing what people are doing there as well as listening to what they say they are doing (Myers, 1999). Central to an ethnographic study is the sense of "being there," "being immersed in the situations, events, interactions and so forth" (Miettinen et al., 2009, p. 1315). In practice, this means that "organizational ethnographers do not study organizations, they study in organizations" (Van Maanen, 2011, p. 221). Consequently, ethnographic research affords the potential to gain a deep understanding of the people, organization, and the wider context. Furthermore, it often leads to findings that significantly differ from corporate or organizational discourse about work (Orr, 1998) and may provide information that challenges the "taken for granted" assumptions (Myers, 1999). Among the reasons why the ethnographic approach is particularly well suited for studying practice (i.e., how InfoSec policy is crafted in this study) and practices, and therefore for this study, are:

1. The flow of practice is temporal;
2. Practices are always situated and immersed in a context; and
3. Practices direct the researcher's attention to the mundane, micro-level aspects of work.

Next, I briefly unpack these three arguments further. First, practices are temporally evolving and open-ended (Schatzki, 2002, p. 87), and actions related to a certain practice unfold in real time and over time. Atemporal accounts of practice fall short as practice always has a direction and a tempo (Bourdieu, 1990), which atemporal accounts miss sight of. Ethnographic study helps to uncover this temporal dimension of practices and activities as the researcher spends a long time at the research site. The ethnographic approach, thus, enabled me to see the phenomenon under study as it "happened." Second, the practice perspective acknowledges the irreducibly situated nature of the reality experienced by the actors (Sandberg & Tsoukas, 2011). Situated actions are, indeed, central to research that draws on the practice theory perspective. Situated actions are actions performed in the context of particular, concrete circumstances such that the actions are always contingent on particular, unfolding circumstances (Suchman, 2007, pp. 26–27). Ethnographic studies are particularly well suited for a study that seeks to understand practices in a context: "Understanding actions and beliefs in their proper context provides the key to unravelling the unwritten rules and taken-for-granted assumptions in an organization" (Myers, 2009, p. 93). The situated actions involved in the InfoSec policy crafting were central for publications I, II, and III. The focus on these was on the relational practices through which the InfoSec policy was accomplished. Third, ethnographic study provides the researcher with first-hand encounters with the actors doing whatever they do in their own, situated contexts (Miettinen et al., 2009). In other words, ethnographic studies focus on "work practice, on what is actually done, and on how those doing the work make sense of their practice" (Orr, 1998, p. 439), and thus offer grounded accounts of practices (Orlikowski, 2002). Therefore, it allowed me to focus on the mundane, micro-level aspects of InfoSec policy crafting – on the doings and what was done in the crafting of the policy. For these reasons, I see ethnography to be well suited and even the privileged mode of inquiry (Rowe, 2012) for this particular study.

3.2.2 A case study approach

The part of this research which focuses on the relationship between InfoSec policy crafting and InfoSec policy compliance (i.e., research question 3 and publication V) draws its empirical material from an exploratory single-case study. The context of the case is Gamma (a pseudonym), an internet service provider. Yin (1989) defines the case study approach as "an empirical inquiry that investigates a contemporary phenomenon within its real-life context when the boundaries between phenomenon and context are not clearly evident and in which multiple sources of evidence are used" (p. 23). Two of the important uses for case studies are to gain inspiration for new theoretical ideas and to illustrate some phenomenon (Siggelkow, 2007). Case studies are further well suited for analyzing change processes, because they enable researchers to study the contextual factors and process elements in real-life situations (Halinen & Törnroos, 2005). They are further suitable for studies that draw on practice theory as evidenced by, for example, Jarzabkowski et al. (2012) in studying coordinating and Smets et al. (2012) in studying how institutional change originates in local, everyday practices.

In light of the above discussion, it can be argued that an exploratory case study is suitable for studying how InfoSec policy crafting is implicated in InfoSec policy compliance for the following four reasons. First, it provides a means for studying a contemporary phenomenon, which cannot be separated from its context, but has to be studied within it to understand the dynamics involved. InfoSec policies are clearly a contemporary phenomenon. Separating their crafting from the context of that crafting would likely only result in an acontextual account. Second, in this study, case study is used as an illustration and as a source of inspiration. That is, the previous analysis of the case data inspired some theoretical ideas that were further developed, and then the case study was used as an illustration in publication V. The purpose of illustration further justifies the selection of a single case instead of surveying many cases. Here, depth and comprehensiveness for understanding the phenomenon outweigh any claims for statistical representativeness. Third, as InfoSec policies should translate into actions (Warkentin & Johnston, 2008), their outcomes should be some form of change in the organization. Case study provides a means for studying related change processes. Finally, case study is in line with the practice theory perspective of this study and the assumptions it brings to studying organizational phenomena.

3.3 A brief description of the research settings and the researcher's role

Practice and practices as an object of the analysis requires deep engagement in the research setting. Consequently, research that studies practices in situ is typically characterized by a rich understanding of situated phenomena, and thus employs a single or a few research settings rather than surveying many. Yet, it can be beneficial to identify "different sites where the same practice is carried out" to achieve a broader and deeper understanding of the phenomenon (Nicolini, 2009b, p. 132). Indeed, this study is multi-sited (Marcus, 1995; Hannerz, 2003; Nicolini, 2009a), which is justifiable by the fact that the practice and practices are multifaceted and multi-dimensional phenomena (Nicolini, 2009a).

The study explores InfoSec policy crafting through three settings: a global engineering corporation (Alpha); a local IT service provider (Beta); and a multinational internet service provider (Gamma). Each setting represents a different type of organization, a different approach to information security management, and a different approach to policy crafting. What connects the settings is the practice of InfoSec policy crafting (cf. Nicolini, 2009b). Together, the settings complement each other and offer a richer foundation for understanding InfoSec policy crafting than any one setting could offer. Yet, the purpose of including three settings is not to compare them (i.e., this is not a comparative study).

The following brief descriptions are based on the situations at the time of the studies. More details about the organizations can be found from the publications included in this dissertation. The names of the companies and participants as well as the key technical details have been disguised in order to protect the confidentiality of the research settings and their members. Because of the sensitive nature of information security for organizations, I go to some lengths to obscure the actual identity of these organizations. I do acknowledge that this results in some ambiguity around issues such as exact dates when the policies were made and when studies began and ended, but it is necessary to maintain the organizations' anonymity.

3.3.1 Alpha

Alpha is a Nordic-based, multinational corporation and one of the world leaders in the field of mechanical engineering. It operates in more than 50 countries around the world. While the corporation is a typical exemplar of the engineering industry, its products are going through a rapid change from traditional machinery to intelligent services connected to and maintained through the internet. Alpha’s information security activities have traditionally focused on information technology (IT) security. The corporation has, for example, invested in technological safeguards such as firewalls and virus protection, and has sought to ensure that its IS are operated by reliable partners. Information security risk management and governance have been less of a priority. Information security practices have varied from country to country because the centralized information security management function has had rather limited resources for overseeing Alpha’s branch offices in different countries. The changes in Alpha’s products together with a recent increase in regulation and skyrocketing media coverage of so called cyber threats pushed Alpha to widen the scope of its view on information security. The means for achieving such a wider scope was the crafting of a new InfoSec policy.

I selected the InfoSec policy crafting project at Alpha for inclusion in this dissertation due to the following reasons. First, it was interesting for the purposes of this study because it involved a total renewal of the policy for an organization whose information security threat environment was undergoing a large reorganization. Second, as the whole policy was renewed, I was able to follow the policy crafting in real time. This was important for building an understanding of how the policy emerged in the crafting.

3.3.2 Beta

Beta is a medium-sized company that provides IT services in Finland. The services include IS development and hosting for systems that process and store sensitive data (e.g., data that are regulated by data protection regulations). Many of Beta’s customer companies have been classified as part of society’s critical infrastructure by the national emergency supply agency. Therefore, information security is a top priority for Beta’s customers and crucial for Beta’s business. Accordingly, Beta has a long tradition in managing information security. At Beta, a project to craft a new InfoSec policy was driven by recommendations from an external assessment and information security professionals’ interest to further improve Beta’s information security. A central tenet of the policy crafting was the utilization of international best practices to improve Beta’s information security.

I selected the InfoSec policy crafting project at Beta for inclusion in this dissertation as it enabled understanding how the challenges of InfoSec policy crafting can be approached in scholarly research and analyzing how information security best practices and local, situated practices interact and translate, and how policy emerges through these translations.

3.3.3 Gamma

Gamma is a publicly listed telecommunications and internet service provider that operates in 20 markets and has its headquarters in the Nordics. It offers network access and telecommunication services both to business and private customers. Due to the type of data processed and stored, and the services provided, Gamma's business operations are highly regulated by various data protection laws and regulations. These, together with customer-mandated information security requirements, make information security a central concern for the organization. The centrality of information security for the organization is reflected in the maturity of Gamma's information security management practices. Because Gamma's comprehensive InfoSec policy had already been in place for some time, Gamma offered a possibility to analyze the relation between InfoSec policy compliance and policy crafting. Therefore, I selected Gamma for inclusion in this dissertation.

3.3.4 Access to the research settings and the researcher's role

This research benefits from the unusual and prolonged access to the research settings of Alpha and Beta. For both settings, I was granted full and continued access to the premises of the organizations and different materials related not only to information security but also to the organizations' strategies, other policies, and ways of working. This unusual access was made possible as I worked as an information security professional in parallel to this research, and was thus a "professionally qualified doctoral student" (Klein & Rowe, 2008). Throughout the research in these settings, I enjoyed privileged resident status, involving open access to facilities and people for the purpose of observation and informal discussions. This comprised access to workshops, meetings (both face-to-face and virtual), and more informal settings. My role in both of these settings was partly consultative as is typical for ethnographic studies (Rowe, 2012). The extent and quality of access allowed for capturing in detail the work on the InfoSec policy (cf. Orr, 1996) as it unfolded in space and time.

To Gamma, another researcher and I had a more common and a more limited access. We were granted access to one office space for the whole time of the study, and access to information security managers' and other information security professionals' meetings over a seven-month period. We were also given a two-day introduction to the work of an information security manager at Gamma. We further had access to company materials related to information security. At Gamma, my role was purely the role of a researcher.

My background as an information security consultant further afforded intimate knowledge of the information security field, including many of its emergent challenges, troubles, and joys. My background further facilitated an understanding InfoSec policy crafting practices at the research settings, because practice is "not only understandable to the agent or the agents who carry it out, it is likewise understandable to potential observers (at least within the same culture)" (Reckwitz, 2002a, p. 250). Together with the extended engagement with the research sites, my professional background provided substantial knowledge and expertise that helped with the analysis and in formulating possible explanations for increasing our understanding of InfoSec policy crafting (cf. Klein & Rowe, 2008).

3.4 Empirical material

The empirical material of this study was constructed through different methods in order to achieve an understanding of InfoSec policy crafting and a solid foundation for theorizing. Analysis of the empirical material was qualitative in all studies included in this dissertation. Theorizing mostly proceeded iteratively between empirical material and the existing literature.

3.4.1 Constructing empirical material

Ethnographic research differs from case studies (Myers, 1999) and other types of interview- or document-based research (Miettinen et al., 2009) by the extent to which the researcher immerses herself in the situations, events, and interactions at the research site. A chief distinguishing characteristic of ethnographic research is, thus, participant observation as a means for collecting empirical material (Myers, 1999). For example, in Orlikowski's (1991) seminal ethnographic study in IS, data was collected through participant observation, informal social contact with the participants, unstructured and semi-structured interviews, and a documentation review. Similarly, drawing on the practice theory perspective requires deep engagement in the field, working with or observing practitioners doing their work (Feldman & Orlikowski, 2011). Indeed, Schatzki (2005) argues that to identify and to understand practices as they occur, "requires considerable 'participant observation': watching participants' activities, interacting with them (e.g., asking questions), and – at least ideally – attempting to learn their practices" (p. 476). Participant observation further overcomes some of the limitations inherent for interviews for accessing practice (Alvesson, 2003). Accordingly, the main method for constructing empirical material for the two ethnographic studies was participant observation. Documentary sources complement the empirical material from the participant observation. For the case study, the sources of the empirical material include semi-structured interviews, non-participant observation, and documentary sources. The empirical material is summarized in Table 3, Table 4, and Table 5 and discussed below.

Participant observation. To reveal the sense in which practices are enacted, participant observation focused on what people actually did, on the activities they were involved in to accomplish particular purposes (Sandberg & Tsoukas, 2011). I chose the InfoSec policy projects as the unit of observation, which allowed me to observe the activities and actors producing policy as the projects unfolded, rather than prejudging which activities, events, or actors might be central for InfoSec policy crafting (cf. Kaplan & Orlikowski, 2013). My daily observations of InfoSec policy crafting included actors' work-around policies, the meetings and workshops they organized and participated in, and the meeting and workshop preparations they made as well as episodes or critical events that influenced their work. I observed people and their actions, but not only them; I paid attention to the materiality of practices. Representing practices without paying close attention to "the landscape of tools, artefacts and resources" that form the part of accomplishing practices and considering what they do and how they make a difference would lead to an impoverished and inadequate account of practices (Nicolini, 2009a, p. 1402). Therefore, I kept close track of different tools, artifacts, and resources that might be critical for the accomplishment of policy crafting. I further asked questions after meetings and other activities to clarify what had happened. Unless the actors were in a great hurry, they were usually happy to discuss their actions and views. As actors provided situation-specific details, I asked relevant follow-up questions to build a deeper understanding of the policy crafting and the actors' role in it.

Participant observations enabled informal social contact with different actors. Informal contact with the people directly associated with the InfoSec policy crafting offered me a means to capture the experience of and the meaning of their actions to the various actors involved as well as practical concerns that governed and affected their actions. Practices feature intentionality (Schatzki, 2001). Therefore, discussion often delved into elements of intentionality inscribed in practices as viewed by the actors. Actors' vocabulary of motives and goals or explanations, justifications, and prescriptions of their actions often helped here (Nicolini, 2009a). Other topics often discussed included: (1) the meaning and value of the InfoSec policy; (2) the practice of crafting the InfoSec policy; (3) the context in which the InfoSec policy was constructed; and (4) the relationship between the InfoSec policy crafting and information security management work.

I noted down and typed up my observations and information from the social contact with the actors and my early interpretations as extensive field notes during and soon after each observation day. I adapted a template for the field notes from Schultze (2000, p. 17). It includes date, location, main events, small or odd events, main actors, a detailed description of the day, and possible early interpretation and personal notes (for an example, see Appendix A: Observation notes template and excerpt from observation notes). In sum, direct, daily observation revealed the micro-level, situated dynamics by which InfoSec policy was made, thus providing the basis for a rich "ethnography of InfoSec policy crafting."

Table 3: Empirical material and use in the ethnographic study 1

Empirical material	Type of empirical material	Use in the analysis
Participant observation	*Field notes from 15-month participant observation.* Detailed record of social interactions, conversations, workshops, meetings, and use of artifacts observed during policy crafting from the early stages until final approval of the policy. *Informal social contact.* Informal talks with information security professionals, chief technology officer (CTO), head of risk management, compliance officer, legal representatives, R&D representatives and chief information officer (CIO) board members, ranging from brief exchanges to longer discussions before and after meetings and workshops and during work breaks.	Produce a description of the project and reveal micro-level, situated dynamics through which policy was crafted, and analyze the collective construction of local InfoSec practices as well as legitimizing strategies of InfoSec policy crafting. Familiarize with the organizational context, gain trust of actors, discuss and clarify project-related issues, and support emerging interpretations. Integrate observations with actors' accounts. Provide opportunities to clarify open matters and challenge the emerging understanding.
Documentary sources	*Company-related documents:* Information management policy, safety policy, privacy policy, intranet materials, and various other organizational documents. *Policy crafting-related documents:* Old InfoSec policy, InfoSec instructions, PowerPoint presentations related to policy crafting, tens of policy drafts, information security best practices (e.g., ISO/IEC 27001 and ISO/IEC/27002).	Familiarize with the organizational context. Support evidence and clarify interpretations from observations and social contact (Smets et al., 2012). Support the identification of the differences between best practices and local documented practices in order to reconstruct changes. Keep record of the outcome of project episodes.

Table 4: Empirical material and use in the ethnographic study 2

Empirical material	Type of empirical material	Use in the analysis
Participant observation	*Field notes from six-month participant observation.* Record of social interactions, workshops, meetings, and use of artifacts during policy crafting from early stages until policy implementation. Record of how situation had evolved from later site visits. *Informal social contact.* Informal talks with information security professionals, CTO, production managers, service managers, and other employees, ranging from brief exchanges to longer discussions before and after meetings and workshops and during work breaks.	Produce a description of the project and reveal micro-level, situated dynamics through which policy was crafted and implemented, and analyze the translation from information security best practices to local practices. Familiarize with the organizational context, gain trust of actors, discuss and clarify project-related issues, and support emerging interpretations. Integrate observations with actors' accounts. Provide opportunities to clarify open matters and challenge the emerging understanding.
Documentary sources	*Company-related documents:* Business strategy, intranet materials, IS strategy and related documentation, and various other organizational documents. *Policy crafting-related documents:* Old InfoSec policy and related documents, PowerPoint presentations related to policy crafting and implementation, several policy drafts, information security best practices (e.g., Finnish standards for InfoSec).	Familiarize with the organizational context. Support evidence and clarify interpretations from observations and social contact (Smets et al., 2012). Support the identification of the differences between information security best practices, local documented practices and what happens in practice to understand the translations of practices. Keep record of the outcomes of project episodes.

Semi-structured interviews. Semi-structured interviews (Kvale & Brinkmann, 2009) were the means for constructing the main empirical material for the case study. They provided a means for understanding InfoSec policies from the point of view of the informants and how the practices of policy crafting were related to policy compliance. Interviews were conducted according to an interview guide (Kvale, 1996) and centered around three themes: (1) InfoSec policies and their relation to informant's work and responsibilities; (2) the value of the InfoSec policies for the informant; and (3) the future of the InfoSec policies. Each interview lasted approximately one hour. All interviews were recorded and transcribed verbatim.

Table 5: Empirical material and use in the case study

Empirical material	Type of empirical material	Use in the analysis
Semi-structured interviews	*Transcriptions from semi-structured interviews.* 19 semi-structured interviews with senior managers, employees responsible for organization's central IS, and InfoSec professionals.	Produce a chronological narrative (Langley, 1999) of how InfoSec policy compliance unfolded, and create a textual account of the practices around policy compliance.
Documentary sources	*Company-related documents:* Annual reports, information from public website, intranet materials. *Policy crafting-related documents:* InfoSec policy and related information security instructions.	Familiarize with the organizational context. Support evidence and clarify interpretations from interviews.
Non-participant observation	*Field notes from non-participant observation.* Record of social interactions during information security professionals' meetings over a period of seven months and a day-long workshop around InfoSec policies as well as a two-day introduction to information security professionals' work at the studied organization. *Informal social contact.* Informal talk with information security professionals and employees.	Familiarize with the organizational context, discuss, clarify, and support emerging interpretations.

Documentary sources and non-participant observation. While field notes from the participant observation and informal social contact constituted the basis for my analysis in both ethnographic studies and transcriptions from semi-structured interviews in the case study, I had access to documentary sources that increased my understanding of the context of the organizations' InfoSec policies (e.g., existing InfoSec policies and related process documents and instructions, minutes of the meetings related to information security, IS strategy, and intranet pages as well as information security management best practice guidelines). For the case study, non-participant observation further helped in familiarizing myself with the organizational context. Describing and understanding the context of the studied phenomenon is crucial not only for ethnographic studies but also for case studies (Klein & Myers, 1999). Documentary sources further clarified some of my interpretations from the observations (Smets et al., 2012).

3.4.2 Analysis of the empirical material

Empirical material from the participant and non-participant observations, semi-structured interviews, and documentary sources provided a solid foundation for tracing the InfoSec policy crafting and its implications to policy compliance. The analysis of the empirical material was qualitative in all studies and involved moving back and forth between the empirical material and the literature in such a way that they mutually informed emergent theoretical insights.

Prior research (e.g., Schultze & Orlikowski, 2004; Jarzabkowski et al., 2012; Smets et al., 2012) has demonstrated how practices can be analyzed and how a practice theory perspective can be used in the analysis to understand complex, dynamic, and unprecedented organizational life. In line with this tradition, I relied on qualitative techniques for analyzing data. While qualitative techniques for analyzing data are plentiful (Miles & Huberman, 1994), the specific techniques I employed include:

1. Writing chronological stories of policy crafting (Langley, 1999) based on observation notes and other empirical materials;
2. Open coding and axial coding of the stories: I read through the stories and marked sentences or passages of sentences with codes that emerged from the data. I analyzed the codes further by analyzing the codes and representative passages in a spreadsheet;
3. Intensive reading of the existing literature, stories, and field notes as well as visualizing empirical material in tables (Miles & Huberman, 1994) and on paper in order to uncover themes; and
4. Analyzing relationships between the uncovered themes.

For example, for publication III that delves into the legitimization of an InfoSec policy, I first wrote a chronological story of policy crafting that uncovered two consistent themes that characterized the crafting: (1) the waning or lacking acceptance and support for InfoSec management and new InfoSec policy; and (2) a corresponding increase in descriptions of events that in one way or another promoted or argued for the policy. After delving into literature on information security management, I came to understand that these themes were underdeveloped in the existing literature. Yet, organization studies provided possible concepts for understanding them (i.e., legitimacy and legitimization). Therefore, I analyzed the story I had written using open coding for incidents of legitimacy and legitimization. This analysis resulted in the first-order codes such as “Lack of authorization,” “Seeking authorization/acceptance for policy,” and “Seeking approval for policy’s practices.” To uncover broader themes, to ensure consistency with the existing literature, and to detect possible new themes, I then built on the first-order codes and coded for similarities and differences between them. Uncovered themes included, for example, “Advertising,” “Inviting participation," "Formalizing and professionalizing," and "Embedding into existing practices." Finally, with the emergent themes in hand, I went back to the original story and other empirical material to map the themes to the dynamics I had uncovered in the description of the policy project. This mapping presented an opportunity to compare dynamics such as increasing or waning acceptance to amendments in the policy draft across different time periods as well as contextual factors (e.g., cultural norms, unexpected internal events) surrounding these dynamics. Eventually, this analysis resulted in an understanding of how legitimacy of the new InfoSec policy, legitimization strategies, and policy amendments interrelated over time, and ascertained the manner in which actors at the studied organization legitimized their new InfoSec policy.

4 FINDINGS

In this chapter, I bring together the findings of this dissertation in light of its research questions. The chapter is structured as follows. First, I summarize the research publications included in this dissertation. Second, I bring together the main findings of this study for each research question.

4.1 Summaries of the research publications

The foundation of this dissertation is composed of five publications. In the following sections, I summarize these publications. The original publications are included in Appendix B Publications.

4.1.1 Publication I: Information systems security policy implementation in practice: from best practices to situated practices

This study was motivated by the observation that, while information security best practices are central to managing organizational information security, their organizational application in practice has been largely absent from the literature. Therefore, this ethnographic study analyzes InfoSec policy implementation as a process of translation from information security best practices to an organizational InfoSec policy and further to situated practices. The findings of the study demonstrate how the organization's employees, their work, and organizational practices are central for the process. In particular, the findings suggest that, on one hand, the translation was inhibited by incongruent practices, insufficient understanding of employees' work, and the information security managers' lack of engagement in organizational practices. On the other hand, allowing situated practices to shape the policy and actively engaging employees in the reconstruction of situated practices contributed positively to the translation. The emergent challenges the organization faced in its implementation efforts were not so much related to crafting an InfoSec policy from the prescriptions of the best practices, but implementing the policy in a way that was sensitive to local ways of working and that was congruent with other organizational practices, such that the policy could become a part of the existing practices and enactable by the employees. The study argues that to craft and implement an InfoSec policy is to translate, and the success of the process is relational to how the translation takes place.

4.1.2 Publication II: Crafting an information security policy: insights from an ethnographic study

This study was motivated by a practical concern that neither research nor industry best practice guidelines address how an organizational InfoSec policy is crafted in practice. Yet, crafting such a policy is a central concern for practitioners. To begin to address this concern, this ethnographic study seeks to understand the crafting of an organization-wide policy in practice and the practices that lead to successful policy crafting. Based on ethnographic evidence from 15 months participant observation, the study illustrates some of the challenges and practices InfoSec policy crafting entails at a global mechanical engineering corporation.

The findings of the study suggest that the key practices amid which an InfoSec policy was crafted at the studied organization were: (1) borrowing information security practices for the InfoSec policy from international information security best practices; (2) inviting in-depth participation in policy crafting; (3) legitimizing InfoSec policy through different strategies; and (4) clarifying the ramifications of the policy implementation. I derived five managerial implications for successfully crafting an InfoSec policy from these practices and the ethnography presented in the paper. These implications advise managers in building the foundation of their InfoSec policy, contextualizing the policy's practices, inviting participation of organizational members to policy crafting, legitimizing the policy, and estimating the ramifications of policy implementation.

While the main motivation for the study was practical, the study affords contributions to research. The study contributes not only by illustrating policy crafting, but also by suggesting how information security best practices can be used in the InfoSec policy crafting and how such best practices can be contextualized. The study further extends the existing research on employees' involvement in information security management by suggesting and describing the active role organizational members play in policy crafting.

4.1.3 Publication III: Legitimising information security policy during policy crafting: exploring legimitising strategies

This study was motivated by the existing literature that argues that InfoSec policies often remain decoupled from organizational practice, which has called for studies that illuminate the emergent process of policy crafting. Drawing on organization theory on legitimacy and legitimizing and on ethnographic evidence, the study examines InfoSec policy crafting as a process of legitimizing. In particular, it seeks to understand how policy becomes legitimized in the policy crafting process and what the implications of legitimizing policy are.

The findings of the study identify four legitimizing strategies employed during InfoSec policy crafting: (1) inviting participation; (2) embedding into existing practices; (3) advertising; and (4) formalizing and professionalizing. The study further conceptualizes InfoSec policy crafting as being constituted through the iterative and recursive relationship of legitimizing strategies and policy amendments. InfoSec policy derived its authority and legitimacy through these successive cycles of legitimization strategies and amendments; policy content became more fixed, less subject to changes, and more authoritative over the course of the policy crafting.

The study contributes to the literature by illuminating the legitimizing processes that extend the theorizing on legitimacy and InfoSec policies. It offers an alternative view on InfoSec policy development by conceptualizing it as a process of legitimization that highlights the emergent process of the policy crafting, and by suggesting that the legitimacy of the InfoSec policy is in part already accomplished during policy crafting and not only after.

4.1.4 Publication IV: A practice lens for understanding the organizational and social challenges of information security management

This study emanated from the calls in the existing literature for a better understanding of the organizational and social aspects of information security management. While the existing literature often depicts information security management as rather linear, systematic, and rationalist process, it has been argued that the complexity, uncertainty, and political nature of managing in real-life situations set the limits on the applicability of such rationalist approaches. In particular, such a view pays little attention to the organizational and social challenges inherent in information security management. Therefore, this study draws on practice theory in order to develop a practice lens for understanding and studying how people, practices, and what happens in practice interact and create such challenges. The lens suggests that information security management emerges as a nexus of practices, actors, and praxis:

- Information security management practices are influenced by shared practical understandings, meanings, and norms in regard to information security that reflect the wider social and organizational practices.
- Actors are the people who perform different activities related to information security and enact its practices. When actors take part in information security, they draw upon available practices from their

organizational and extra-organizational context. The actors likely include not only information security professionals but also other organizational members (for example, business managers, risk managers, and external consultants).

- What actors actually do is information security management praxis that includes a multitude of activities involved in organizing information security. It may entail political gambles for executive buy-in, accommodating conflicting views of shareholders, or responding to unexpected events. It is not only influenced by the practices but also by the situational contingencies where the praxis takes place.

I elaborated and illustrated the lens through an ethnographic study that analyzed the development and implementation of an InfoSec policy at an IT service provider. The analysis revealed that the social and organizational challenges of InfoSec policy crafting were related to: (1) conflicts between the practices employed by information security professionals and employees' expectations; (2) conflicting understandings between information security professionals, employees, and the organization's management; and (3) information security professionals' inadequate understanding of employees' work. Further, situational events shaped the policy development and implementation. The challenges and events hindered the policy crafting.

The practice lens offers an alternative to the existing accounts of information security management by describing how people, practices, and what happens in practice interact and create organizational and social challenges. It contributes to the literature by providing content to the abstract phases of InfoSec policy development suggested in the existing literature. Specifically, the lens highlights that the "content" is created by actors, practices, and what happens in practice, and facilitates the analysis and identification of the role of individual actors, social structures, and situational events in this process. The lens further contrasts with the existing accounts by highlighting that the information security management process likely interacts with and is influenced by other social processes happening in an organizational context. Particularly, the longitudinal perspective of the lens revealed how implementation of the InfoSec policy proceeded from an initial decision through various modifications into final implementation. The implementation was connected to other processes occurring at the organization during the implementation. Finally, the lens suggests that researchers should focus more on what actors do (i.e., their praxis) as opposed to what they should do (e.g., prescriptions of information security management standards) or what they aspire to do. The lens affords a theoretical framework and a vocabulary for such an endeavor.

4.1.5 Publication V: Enacting information security policies in practice: three modes of policy compliance

Literature on InfoSec policy compliance has predominantly focused on identifying (socio-) psychological factors that anticipate employees' policy compliance. Such research has overly focused on the mental over the material and policies, as "material objects" have become invisible in policy compliance studies. Therefore, this study focuses on the relationship between materiality and policy compliance. We first theorize the relationship by building on sociomaterial theorizing and on the concepts of reification and fetishization. We then elaborate and illustrate the theorizing through a case study about InfoSec policies at an internet service provider.

The findings of the study illustrate that through practices of reification, "information security" materialized iteratively into a set of documents into an InfoSec policy. Through various practices that exalted, extolled, and celebrated the policy, the material policy acquired qualities that were not reducible to its material form. The findings further uncovered three modes of policy compliance in which compliance is relational to policy creation (reification) and celebration (fetishization) practices: (1) spirit; (2) consensus; and (3) objectual. In the first mode of compliance, "compliance as spirit," policy as a material "object" was not present as such but as a material referent. In the second mode, "compliance as consensus," compliance was not relational to the enactment of the documents per se in the practices, but it was a consensual practice in which policies were implicated as a mutual agreement or enacted through a human proxy. Finally, in the last mode of compliance, "compliance as objectual," the policy documents were implicated in the enactment of practices; they were physically present.

The analysis presented in the paper reveals a more complex picture of InfoSec policy compliance than has been acknowledged in the existing literature, and which seems more truthful to the unfolding of policy compliance in practice. The analysis suggests that policy compliance unfolds differently across practices. That is, as the policies become implicated in the enactment of practices differently, the policy compliance surfaces differently across practices (i.e., the mode of policy compliance varies). Therefore, rather than evaluating policy compliance as universal, it should be viewed as a matter of evaluating the enactment of practices in relation to the mode of compliance. Viewing policy compliance as a matter of enacting practices implies a shift from intentions to complying with doings. In other words, the findings of the study suggest that policy compliance is not a matter of thinking, neither any non-action, but it is in the action of complying. Based on the findings of the study, we argue that policy compliance should not be viewed in isolation of the materialization of policies in the enactment of practices in practice.

4.2 Addressing the research questions

In the following sections, I summarize the findings of this dissertation in light of its research questions. More specific findings can be found in the publications included in this dissertation.

4.2.1 RQ1: How can the challenges that surface during the crafting of an organizational information security policy be studied?

The research question aims at understanding how the challenges that surface during the crafting of an InfoSec policy can be approached in scholarly research. In line with the overall focus of the study, I approached this question from the perspective of practice – from the actual accomplishment of InfoSec policy crafting. Consequently, the challenges are those problems that surface in the practice of doing (i.e., they are emergent). The findings of the study suggest that studying the challenges that surface during the crafting of the InfoSec policy necessitates the following:

- Theories about situated performances of InfoSec policy crafting in contrast to prescriptive theories that abstract policy crafting as a set of policy development phases;
- Acknowledging and accounting for emergence in InfoSec policy crafting in contrast to prescribing mechanistic processes of InfoSec policy development; and
- Research methods that enable deep engagement with the everyday realities of the InfoSec policy crafting, and that enable observing practices of InfoSec crafting with all its contingent, emergent, and multiplicitous nature.

In the following, I detail these three findings. First, studying the challenges of InfoSec policy crafting calls for a theoretical lens that can account for the situated performances of InfoSec policy crafting. In general, practice theories focus on relationships, dynamics, and enactment, and are thus particularly prominent for analyzing situated, novel, and emergent organizational phenomena (Feldman & Orlikowski, 2011). This study suggest that practice theories (see, for example, Schatzki, 2001) might provide a foundation for theoretical lenses for understanding InfoSec policy crafting. In publication IV, I developed a practice-theory based lens for understanding and studying the challenges of InfoSec policy crafting and information security management more broadly. This lens adapts and uses practice theory in the context of the InfoSec policy development and depicts information security management as emerging from situated information security management work and from the enacted social structures of and events arising at the organization and its environment. A key for attempting to understand the challenges is, thus, in seeking to understand how people, practices, and what happens in practice interact and create the challenges. By suggesting a focus on what is actually done in accomplishing an InfoSec policy, the lens contrasts with prescriptive theories that abstract policy crafting as a set of policy development phases (see Section 2.1.2).

Second, studying the challenges of InfoSec policy crafting highlights the need of acknowledging emergence in the crafting. In contrast to what mechanistic, systematic, and linear processes of policy development might hint at (see Section 2.1.2), a practice lens (publication IV) suggests that the complexity and uncertainty of real-life settings imply that policy emerges rather than formulated. That is, policy is not simply formulated through some predetermined phases, but it emerges as policy crafting happens. As evidenced by publication I, such a view (i.e., InfoSec policy as emerging in the InfoSec policy crafting) entails an ontological reversal from an understanding of information security practices as largely stable entities, describing specified roles and responsibilities for actors and activities that change when a new InfoSec policy prescribes them to change, to an understanding of the continuous process through which these practices emerge through enactment in practice. In other words, mere changes in the description of a policy will likely only decouple what organizations say they do from what they do. It is rather the implication of these policies in organizational practices that brings the documented practices into being and gives them definitive form and content (see publication V and RQ3).

Third, the findings of the study suggest that studying the challenges of InfoSec policy crafting entails certain kinds of research methods. This finding is related to the aforementioned findings, because drawing on practice theories and acknowledging emergence in the InfoSec policy crafting likely necessitates research methods that afford accessing practice. Accessing real-time practice is, however, always difficult as practice constitutes the scarcely notable and unspoken background of everyday life. Practices have to be “drawn to the fore, made visible and turned into an epistemic object in order to enter discourse” (Nicolini, 2009a, p. 1392). Publications I, II, and III empirically illustrate that participant observation is a viable research method for accessing the practice of policy crafting. While survey studies (and likely other quantitative studies) could produce lists of challenges organizations face when crafting InfoSec policies, participant observation supports an investigation of “becoming” instead of what “is” (e.g., a static list), and may thus lead to a more elaborate understanding of the challenges.

Publication I illustrates how these three findings – theories about situated performances, acknowledging emergence, and participant observation – are relevant and can lead to new insights when brought together. The publication suggests, for example, that incongruence between the InfoSec policy draft and organizational practices, information security professionals' insufficient understanding of employees' work, and their lack of engagement in organizational practices inhibited the translations from information security best practices into InfoSec policy and to situated practices, and constituted an impediment to the policy crafting. In a different context, publication II uncovers different kinds of challenges of InfoSec policy crafting:

- How to create information security practices to be included in the policy;
- How to build legitimacy for policy crafting;
- How to ensure policy's practices fit the organization;
- How to build legitimacy to policy's practices; and
- How to ensure policy is approved by the top management.

Overall, these findings indicate that InfoSec policy is likely modified in response to the challenges of policy crafting during that crafting. How policy emerges in the crafting is the theme of the second research question.

4.2.2 RQ2: How does an organizational information security policy emerge in the crafting of the policy?

The findings of the study suggest that the InfoSec policy emerges in the crafting of that policy as follows:

- Through translations of information security best practices and of situated practices;
- Amid practices that enable the translations; and
- Over policy development phases found in the existing literature.

First, the findings suggest that InfoSec policy emerges through translations of information security best practices and translations of situated practices, such that the best practices and situated practices mingle in the emergent policy; they are brought together in the emergent policy without totally losing their identity. The findings of publication I indicate that, in the crafting of the InfoSec policy, some information security best practices are translated into an InfoSec policy. Translation builds on the assumption that "a thing moved from one place to another cannot emerge unchanged: to set something in a new place or another point in time is to construct it anew" (Czarniawska, 2009, p. 425). That is, the meaning of "translation" in this context far surpasses the interpretation in linguistics, where translation would merely equate with substituting foreign words with their local equivalents (Czarniawska & Joerges, 1996). It points to movement and transformation. Consequently, when information security best practices are translated to become a part of an organizational InfoSec policy, they will not emerge unchanged. An organization's existing situated practices (e.g., how people are used to working) also shape the emergent policy, and some elements of an organization's situated practices are translated into the policy.

Second, the findings suggest that the policy emerges amid practices that enable the translations from best practices and situated practices to the emergent policy. In this study, I conceptualized the practices as follows:

- *Borrowing information security practices for the InfoSec policy from international information security best practices*. Publication II shows how the first versions of the information security practices written in the emergent policy were defined by borrowing them from international information security management standards and by making small changes to the borrowed practices. This practice of borrowing information security practices built a foundation for the emergent policy.
- *Inviting in-depth participation in policy crafting*. Publication II further shows how the emergent InfoSec policy was iteratively amended by contextualizing the information security practices that had been borrowed from the international standards through in-depth involvement of different organizational members. The practice of inviting in-depth participation resulted in that policy's practices being adjusted, modified, and some removed as well as new practices being created and included in the policy. The policy itself emerged towards being more acceptable and more feasible to be turned into actions. The findings of publication I support this finding by emphasizing that the organization's existing practices should be allowed to shape the policy, which in turn necessitates participation from various organizational members in policy crafting.
- *Legitimizing InfoSec policy through different strategies*. Publication III illustrates how the practice of legitimizing InfoSec policy shapes the emergent policy when policy is amended as deemed necessary to legitimize it over the course of policy crafting. As the legitimacy of the emergent policy increased over successive cycles of amendments and legitimization strategies, policy content became more fixed and less subject to changes.

While other practices can be identified in other contexts, the practices identified herein were the practices enacted at the studied organizations. Moreover, other practices were identified in the publications included in this dissertation (e.g., "Clarifying the ramifications of the policy implementation" in publication II, and reification and celebration practices in publication V), but these had less impact on the translations.

Third, the findings show that an InfoSec policy may emerge not only during the "policy development" phase of the existing policy development methods (see Table 2), but also during the "policy implementation phase" and even after it. Publication I illustrates how InfoSec policy took shape after information security professionals had considered the policy "developed" and began to implement it.

Indeed, policy implementation efforts started an iterative reconstruction of the policy in light of information security best practices and the organization’s situated practices, such that the policy was developed and implemented (to use the terminology found in the existing literature) in cycles. Indeed, the InfoSec policy emerges further when it is enacted in practice as the following discussion under RQ3 demonstrates.

4.2.3 RQ3: How is the crafting of an organizational information security policy implicated in policy compliance?

The general starting point for this dissertation was the assumption that InfoSec policy crafting influences InfoSec policy compliance. The findings of the study suggest that InfoSec policy crafting is implicated in—plays a part in constituting—InfoSec policy compliance in the following two ways:

- InfoSec policy crafting may advance policy compliance by bringing an organization’s situated practices and InfoSec policy closer towards each other; and
- How InfoSec policy compliance materializes in the enactment of that policy in the situated practices is relational to the practices of the InfoSec policy crafting.

First, InfoSec policy crafting is implicated in InfoSec policy compliance when policy crafting practices bring an organization’s situated practices and InfoSec policy towards each other. By bringing the practices closer together, crafting practices may facilitate policy compliance. Publication I illustrates that, during policy crafting, an organization’s situated practices shaped the emergent policy and policy crafting shaped the organization’s situated practices. That is, policy and what happened in practice were mutually implicated in each other’s creation. The publication shows that policy was iteratively reconstructed in light of the situated practices, and situated practices were gradually reworked in light of the emerging policy. Such a mutual implication is in line with other practice theory-based accounts that often highlight the reciprocal and mutually constitutive nature of the social phenomena (Feldman & Orlikowski, 2011). Similarly, publication II suggests that the practice of inviting in-depth participation in policy crafting (see also RQ2) shaped the emergent InfoSec policy and made it more compatible with the organizational practice. For example, some content was removed from the policy as the participation uncovered that implementing it would be difficult, costly, and time consuming; in practice, it would never be implemented or complied with.

Second, the findings of this study suggest that how InfoSec policy compliance materializes in the enactment of that policy in the situated practices is relational[2] to the practices of InfoSec policy crafting. This means that InfoSec policy compliance is a plurality that is relational to the policy crafting practices. Publication V builds on the assumption that an InfoSec policy is the result of practices of its crafting (see also RQ2). It identifies three modes of policy compliance relational to the policy crafting practices. It shows that in each mode, the policy compliance becomes articulated differently, and that the articulation is relational to the policy crafting. For example, in one of the modes, "compliance as consensus," compliance appears as a consensual practice that is relational to the policy crafting, which has made the policy largely ambiguous and adaptable. That is, policy crafting had been directed by the principle that policy has to be widely applicable – the policy was to provide guidance to any situation at hand. Furthermore, policy crafting had resulted in policies stored in the organization's intranet, which was also implicated in policy compliance. Storing policy in the organization's intranet meant that policy was "lost somewhere." It was difficult to find. Policy compliance emerged as a consensual practice where acceptability of a certain action in light of the policy was consensually defined. Publication I, supports these findings by showing how policy gradually concretized in relation to particular enactments in practice.

Taken together, these two findings indicate that InfoSec policy compliance begins to emerge during policy crafting and not only after, as is often assumed in the literature (see Section 2.1.1). InfoSec policy crafting practices should not be seen as something separate from policy compliance, but should be taken as something that shape and are inherent in the enactment of situated practices.

Together, the findings to the three research questions provide important insights into understanding InfoSec policy crafting. When viewed from the practice theory perspective, InfoSec policy development and implementation emerge as InfoSec policy crafting. In the next chapter, I discuss these insights and set them in the context of the existing literature.

[2] The intended meaning of the term relational here is what practice theorists understand as the following: "phenomena always exist in relation to each other, produced through a process of mutual constitution" (Feldman & Orlikowski, 2011, p. 1242).

5 DISCUSSION

Despite all the discussion on the importance of the InfoSec policy for organizations and InfoSec policy compliance, one conversation is notably but a murmur: what do people do when they accomplish an InfoSec policy? Amid the studies on importance and compliance, this work (i.e., InfoSec policy crafting) has almost disappeared from sight in scholarly discourse. This has happened despite the increasing importance of information security management for organizations and the coinciding quest for understanding managerial in situ work and practices in other fields of study. How can organizations reasonably craft InfoSec policies without understanding what crafting entails? The obvious answer is that they cannot. Yet, organizations must try. Against this theoretical and practical backdrop, the purpose of this study was to *increase our understanding of the crafting of organizational InfoSec policies*. The findings of the study increase our understanding about:

- How the challenges of InfoSec policy crafting can be studied
- How an InfoSec policy emerges in the policy crafting
- How InfoSec policy crafting is implicated in policy compliance

The chapter is structured as follows. First, I will integrate the findings to present the emergent understanding of InfoSec policy crafting that arises from this study and discuss the study's implications to theory. Second, I will suggest some implications for practice.

5.1 Implications to theory

The findings of this study contribute to the literature on InfoSec policies and on information security management. When brought together, the findings portray InfoSec policy crafting as emerging in the lived contradictions between international information security best practices (i.e., institutional "rules of the game") and local organizational practices, and illustrate how these contradictions are practically and temporarily resolved through crafting (see Figure 5). This new understand about InfoSec policy development was possible due to the present study's focus on how InfoSec policies are accomplished in practice.

Figure 5 integrates the findings of the study. It illustrates that cross-pressures from the best practices and organizational practices create challenges that InfoSec policy crafting has to resolve. It further illustrates that InfoSec policy emerges through translations of the best practices and organizational practices, amid practices that enable the translations. In this study, borrowing information security practices, inviting participation, and legitimizing the policy emerged as central practices for the policy crafting. Through these practices, the best practices and organizational practices became translated into the policy and from policy to organizational practice. InfoSec policy crafting is reflected in policy compliance when crafting aligns the policy and organizational practices.

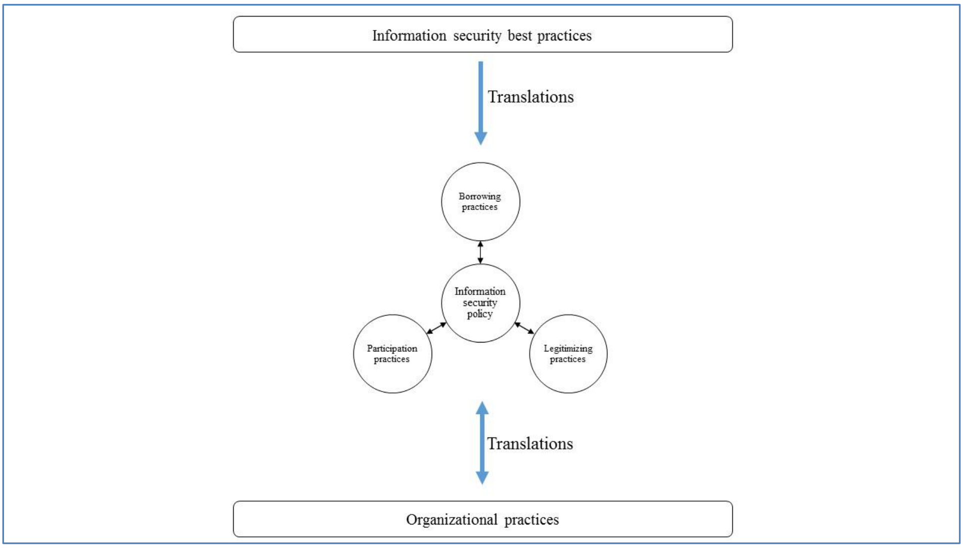

Figure 5: Information security policy crafting

Next, I will discuss the contributions of the study in relation to the existing research (see Table 6 for a summary). As mentioned before, the findings of this study suggest that InfoSec policy emerges in the InfoSec policy crafting through translations and enabling practices, and not only during policy development but also during policy implementation and when policy is enacted in practice. Understanding how InfoSec policy emerges in the policy crafting contributes to InfoSec policy literature by theorizing how and why policy is modified in the course of policy crafting, and explains why some policy drafts persist and others change. In particular, it extends research on developing InfoSec policies in organizational contexts by suggesting the field of practices as the arena for studying InfoSec policies in contrast to power relationships (Lapke, 2008; Lapke & Dhillon, 2008; Kolkowska & Dhillon, 2013) or contextual factors (Karyda et al., 2005). As the following discussion illustrates, this approach resulted in further contributions.

Table 6: Summary of the main new knowledge and its relation to the existing research

Research focus	New knowledge from the present study	Relation to prior knowledge	Contribution of the present study
InfoSec policy development	The challenges that surface in the practical accomplishment of the InfoSec policy development (i.e., in crafting) can be studied: • Through theories about situated performances; • By acknowledging emergence in policy development; and • Through participant observation.	A key issue in both research and practitioner-oriented literature is that they are primarily concerned with the questions of *what*, while abstracting from the question of *how* InfoSec policy is accomplished in certain contexts. Prior research on InfoSec policy development has been primarily concerned with: • Universal methods or contextual accounts (see Figure 3); and • Located challenges of InfoSec policy development in developing universal abstractions (e.g., Rees et al., 2003; Whitman, 2008; Knapp et al., 2009; Flowerday & Tuyikeze, 2016), or in identifying contextual issues such as power relationships and values (e.g., Karyda et al., 2005; Lapke, 2008; Lapke & Dhillon, 2008; Hedström et al., 2011).	The present study provides researchers with: • A means to study InfoSec policy development in situ to analyze how InfoSec policy development unfolds; and • A means for approaching challenges of the InfoSec policy development that only surface in the doing of the policy.
	When analyzed as a practical accomplishment, InfoSec policy development appears as crafting; as an emergent and situated process in which policy development, implementation, and emerging policy compliance merge into a fluid, multilevel process of translations and involvement through which policy evolves.	Existing research has largely approached InfoSec policy development as: • A rather mechanistic; • Systematic; and • Linear following of certain policy development phases (e.g., Whitman, 2008; Knapp et al., 2009; Flowerday & Tuyikeze, 2016).	The present study contrasts with the existing accounts by arguing that: • InfoSec policy development cannot be understood only as the product of a rote procedure following some abstract phases; and • InfoSec policy development should be understood as a practical, joined, and skilled accomplishment – a craft.

InfoSec policy implementation and information security best practices	InfoSec policy crafting unfolds through contradictions between international information security best practices and local organizational practices that need to be locally resolved.	Prior research has emphasized the importance of international information security best practices for organizational information security (e.g., Hsu et al., 2012). Empirical studies have explained the challenges of implementing best practices by: • Power relationships (Backhouse et al., 2006; Smith et al., 2010); and • Incongruent frames of reference of the participating actors (Hsu, 2009).	The present study extends research by arguing that: • Clashes between what is mandated by the best practices and what is expected by the organizational practices explain the challenges; and • Resolutions to the contradictions are contextual; they cannot be deduced from best practices.
	InfoSec policy emerges through translations of the best practices and organizational practices, amid practices that enable the translations.	Prior research: • Indicates why organizations adopt information security best practices (Hsu, 2009; Hsu et al., 2012); • Highlights the importance of the best practices for organizational information security; and • Stresses that the top-down approach to policy crafting does not work in contemporary organizations (Kirlappos et al., 2013).	The present study argues that: • InfoSec policy emerges in-between the best practices and organizational practices and that both best practices and organizational practices are translated; and • InfoSec policy's practices are neither a copy of the best practices nor do they resemble the situated practices of the organization as they were before the policy crafting.
InfoSec policy compliance	How InfoSec policy compliance materializes in the enactment of that policy is relational to policy crafting practices.	Non-compliance to the InfoSec policy as an outcome of policy development is a major concern in the existing literature. Existing research has primarily: • Approached InfoSec policy compliance from the perspective of employees' intention to comply with the policy (e.g., Warkentin & Willison, 2009; Siponen et al., 2010; Vance et al., 2012; Johnston et al., 2015; Johnston et al., 2016); and • Assumed the existence of the policy without considering how policy development may be implicated in the compliance.	The findings of the present study are new in the InfoSec policy literature and extend research on InfoSec policy compliance by suggesting that the roots of the policy compliance are in the policy crafting.
	InfoSec policy crafting promotes policy compliance when crafting aligns the policy and organizational practices.		

Prior research indicates that organizations increasingly face immense institutional pressures to adopt information security best practices in their InfoSec policies (Hsu et al., 2012). This study shows that they also face pressures from organizational practices to modify the policy to make it enactable in the organizational practices. This is the irreducibly situated nature of the reality people experience (Sandberg & Tsoukas, 2011) where situated action and societal context are closely linked (Whittington, 2006). It is as if the best practices would govern the InfoSec policy crafting from one side and the organizational practices from another. These practices constitute the conditions of possibility for InfoSec policy crafting practices (cf. Korica et al., 2017). This means that policies cannot be made by only relying on best practices. When interpreted through practice theory, it means that InfoSec policy crafting practices, though local, are informed by broader practices by overarching institutional logics (cf. Lounsbury & Crumley, 2007) of the best practices. Those practices are, in this sense, the material enactments of institutional logics (Sahlin & Wedlin, 2008).

This study brought the concept of translation to information security literature. The concept serves to describe and explain how policy's practices emerge from the best practices and organizational practices. Best practices cannot be applied directly in an organizational context and organizational practices cannot be directly copied to the policy. In the policy crafting, some practices are privileged over others, and some are refined and modified. This means that information security practices of the emergent policy are neither a copy of the best practices nor do they resemble the situated practices of the organization as they were before the policy crafting. Rather, they are a result of the reciprocal relationship between the best practices and organizational practices. The reciprocal relationship may further explain some of the issues organizations face in implementing information security best practices that have previously been attributed to power relationships and incongruent frames of reference of different actors (cf. Hsu, 2009; Smith et al., 2010; Niemimaa et al., 2013).

The present study contributes by suggesting that the practices of borrowing information security best practices, inviting participation in policy crafting, and legitimizing the policy describe and explain how InfoSec policy's practices emerge. Through these practices, InfoSec policy absorbed those contextual nuances of the studied organizations that could never be directly derived from, for example, international information security management standards (Siponen, 2006), but that are necessary for an enactable policy (i.e., policy that can be complied with within the given organizational reality). Thus, the theorization of these practices as the enabling mechanisms through which information security best practices become contextualized in the InfoSec policy contributes to literature that has noted that information security best practices have to be contextualized before they can be applied in organizational contexts (e.g., ISO/IEC, 2013;

ISO/IEC, 2013). That is, they "should be translated and transformed to the current work practice when such parts are included in the information security policy" (Karlsson et al., 2017, p. 274).

Whereas previous research has offered insights into why organizations attend to and adopt information security best practices – for example, due to coercive, mimetic and normative isomorphism (Hsu, 2009; Hsu et al., 2012) – the practice of borrowing practices from information security best practices sheds light on how the adoption happens in particular organizations. To borrow practices is not just to copy, but also to change and to innovate. That is, practices are not ready-made and unchangeable but subject to repetitive translation (Sahlin & Wedlin, 2008). Borrowing practices is, in this sense, similar to imitation of institutional ideas that has been conceptualized as performative (Sevón, 1996), which is in contrast to diffusion that has connotations of passive recipients of practices. Borrowing practices is an active process. This further means that as best practices are borrowed and translated, they begin to evolve differently in different settings. Therefore, the adoption of the best practices in different contexts may not lead to total homogenization of the practices.

The practice of inviting participation to the InfoSec policy crafting provides new insight into the important role of participation in information security management. A previous analysis of modern information security development approaches suggests that future development approaches should encourage employee participation, because employee input and knowledge on information security are valuable and because participation promotes social acceptance of information security techniques and procedures (Siponen, 2005). Employees' participation in the InfoSec policy development has been further argued to be one of the critical contextual factors for a successful policy outcome (Karyda et al., 2005). The findings from this study support these arguments. On the surface, the participation seemed to bring forth numerous obstacles to policy crafting. For example, it uncovered incongruence between the policy draft and organizational practices, bringing forth practices that could never be translated into practice due to technological infrastructure inertia or infeasible costs, and highlighting the waning interest in the organization's policy initiative on the part of organizational members. Yet, in the end it enabled iterative reconstruction of the policy draft and the gradual reworking of organizational practices in light of the policy.

The practice of inviting participation illustrates how and why InfoSec policy is modified in the course of policy crafting. From the practice theory perspective, how actors that participate in a certain practice arrange their doings and sayings depends on the enacted practices. To enact a practice is to use it as a resource (Barnes, 2001) and to act out its elements such as acceptable ends and practical understandings (Schatzki, 2005). Based on the findings of this study, it seems that organizational members (i.e., employees, managers, executives) who participate in the policy crafting seek to understand the meaning of the policy to their work. They may realize that the adopted best practices are in conflict with their work practices or hinder their work or the workings of the organization. When they are given the possibility to influence the policy and the policy is modified accordingly, contradictions become alleviated. At the same time, their understanding of the policy and its purpose increase. Their participation and the legitimizing practices make the policy more legitimate. Their participation further affords information security professionals a more realistic picture of the organization’s inner workings and sheds light on what is feasible to include in the InfoSec policy in the given organization. Consequently, this study provides support to the previous argument that developing policies in a top-down fashion through control and enforcement may simply fail, because in modern organizations, employees are used to collaborating and showing initiative. Therefore, they should be the principle agents who decide how InfoSec policy is implemented in specific contexts (Kirlappos et al., 2013). InfoSec policy’s practices do not emerge in a vacuum but are actively translated in the context of organizational practices.

Theorizing legitimizing practices in the InfoSec policy crafting is a new contribution in information security research. In this study, policy emerged through the iterative and recursive relationship of legitimizing practices and policy amendments. Understanding legitimization practices is important as without legitimization, policies may remain decoupled from organizational practice and as symbolic gestures that are unlikely to improve an organization’s information security risk management (Spears et al., 2013). Management and organization studies further indicate that organizational policies that are perceived as illegitimate by organizational members are often decoupled from organizational practices (e.g., Bromley & Powell, 2012; Dick, 2015). Whereas information security research has sought to find ways to promote InfoSec policy compliance as a means for overcoming the decoupling after the policy has been implemented, legitimizing practices contribute to understanding decoupling already during policy crafting. In light of this study, unless changes in the organizational policies and practices are viewed as more legitimate than the prevailing ones, it is not feasible to expect policy compliance but coercion and conflict. Therefore, legitimization practices can be assumed to be important for information security management research more broadly.

According to the findings of this study, InfoSec policy crafting challenges can be understood by acknowledging emergence in the policy crafting, explained by drawing on practice theories and empirically analyzed through research methods that afford deep engagement with the research setting. This new understanding directs attention to how policy crafting unfolds in practice in particular contexts, and therefore extends the existing research that has focused on prescribing universal policy development methods (e.g., Whitman, 2008; Knapp et al., 2009;

Flowerday & Tuyikeze, 2016). A similar criticism that has been attributed to information security best practices that are meant to be universal – they focus on the existence of the particular processes and not their content (Siponen, 2006) – can be attributed to the existing policy development methods. Those as well focus on the process but not on how the process unfolds in practice. Based on the findings of this study, it can be argued that such methods are at "the level of perception" (cf. Ciborra, 1997). They deal "with sanitized, unworlded entities, that have not passed the test of being fully immersed in the world. They miss the chance of getting their hands dirty with the everyday practicalities of organization. Hence, the almost ubiquitous gap between the models and the blurred business world." (Ciborra, 1997, p. 73) Abstraction from a detailed examination of InfoSec policy crafting practices obscures the situated challenges and practical and temporal resolutions of the InfoSec policy crafting. When analyzed empirically by following the policy makers, and as an investigation of "becoming," a different picture emerges. Policy development appears as crafting. That is, it appears as an emergent and situated process in which policy development, implementation, and emerging policy compliance merge into a fluid, multilevel process of translations and involvement through which the policy draft evolves.

The understanding of policy crafting as translations and through enabling practices (Figure 5) contributes to the stream of research that is interested in policy development methods by providing a complementary rather than an alternative view on policy development. In the existing research, InfoSec policy crafting is commonly referred to by suggesting policy development methods that assume a rather mechanistic process; which the actors should learn and follow. This study, in contrast, suggests that InfoSec policy development cannot be understood as the product of a rote procedure following some abstract phases. Thus, describing how policy comes into being as a set of phases that flow linearly or as a "formulation" may imply misleading connotations. It may further lose sight into situated issues that are rendered visible when one zooms in to such phases and to what "formulation" actually entails. The activities constituting policy crafting that I studied were more elaborate and nuanced than the prescribed InfoSec policy development methods. Consequently, the practitioners in this study had to muddle through challenges and sought novel ways to accomplish the policy. By acknowledging the emergence and situated nature of policy crafting, the challenges that are hidden/exist behind the abstract descriptions and that surface in the actual accomplishment of the policy may be revealed.

This study contributes to research on InfoSec policy compliance (e.g., Warkentin & Willison, 2009; Siponen et al., 2010; Vance et al., 2012; Johnston et al., 2015, 2016) by showing that how compliance materializes in the enactment of that policy in the situated practices is relational[3] to policy crafting practices. The relationality of the crafting to compliance is in line with the practice theory, as for practice theory, "the 'breaking' and 'shifting' of structures must take place in everyday crises of routines, in constellations of interpretative interdeterminacy and of the inadequacy of knowledge with which the agent, carrying out a practice, is confronted in the face of a 'situation'" (Reckwitz, 2002b, p. 255). Further, in the crafting, policy's practices and organizational practices mutually constitute each other: organizational practices produce the policy and policy produces the organizational practices. Therefore, crafting is also consequential to policy compliance as it may reconstitute organizational practices, making them more aligned with the emerging policy. While the existing literature seeks ways to promote compliance after the policy has been developed as an afterthought, this study suggests that compliance should be attended to already during development. Based on the findings of the study, I argue that InfoSec policy crafting is of more significance to policy outcomes than is often assumed.

Through introducing ethnography to information security research, this study makes a methodological contribution. While an ethnographic approach has seldom been used in information security research, the study highlights its value in providing both theoretical and practical contributions to the field of information security research. In particular, the study shows that ethnographic approach is relevant for studying information security management practices. The approach allows for analyzing practices as they are accomplished at particular places and times and in a given historical and material context. It further has potential for addressing the calls for more critical information security research (Siponen, 2005a, 2005b), because it can lead to findings that differ from organizational discourse (Orr, 1998) and that challenge the "taken for granted" assumptions (Myers, 1999).

5.2 Implications for practice

Crafting an InfoSec policy is a central concern for organizations and often an arduous and demanding endeavor organizations cannot afford to skip. The concern is accentuated by the ever-complex information security risks, increasing information security and privacy breaches, and increasing regulatory demands for protecting information. By increasing our understanding of InfoSec policy crafting, this study offers implications for practice that might help organizations in this endeavor. As a whole, the study argues that how InfoSec policy is crafted

[3] The intended meaning of the term relational here is what practice theorists understand as the following: "phenomena always exist in relation to each other, produced through a process of mutual constitution" (Feldman & Orlikowski, 2011, p. 1242).

matters; copying the policy from the internet may suffice for complying with information security best practices (i.e., the organization should have an InfoSec policy), but will likely only result in decoupling the policy from the organizational practice.

Four implications for InfoSec policy crafting that result from this study are as follows (see Figure 6):

- Be aware that a likely clash between the prescriptions of international information security best practices and organizational practices creates challenges to InfoSec policy crafting.
- Overcome the challenges by translating both international information security best practices and organizational practices in the policy crafting.
- Utilize the practices of borrowing from information security best practices, inviting in-depth participation of selected stakeholders, and legitimizing by translating international best practices and organizational practices in the policy crafting.
- Recognize that the foundation for InfoSec policy compliance is built during policy crafting. Translating policy to organizational practice begins during crafting.

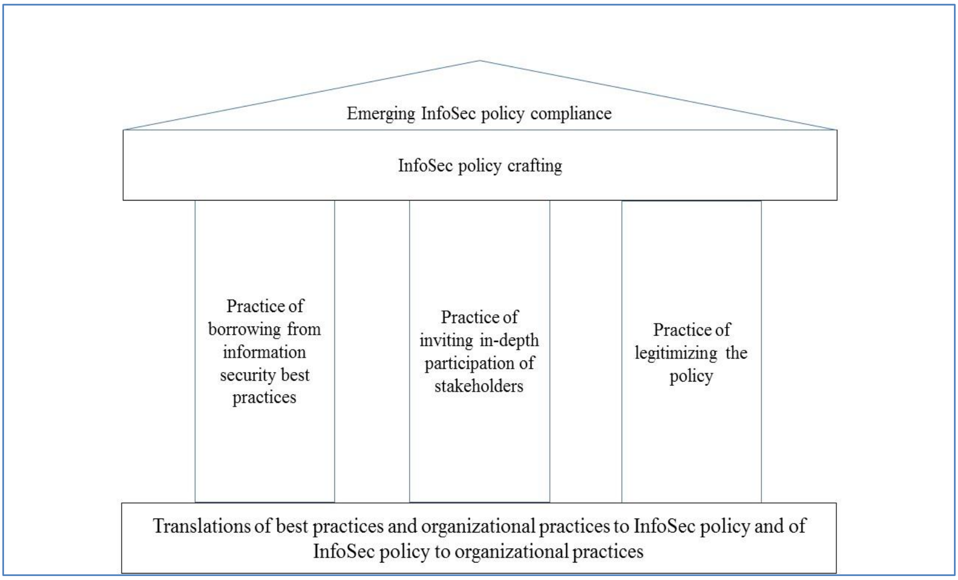
Emerging InfoSec policy compliance
InfoSec policy crafting
Practice of borrowing from information security best practices
Practice of inviting in-depth participation of stakeholders
Practice of legitimizing the policy
Translations of best practices and organizational practices to InfoSec policy and of InfoSec policy to organizational practices

Figure 6: The three pillars of information security policy crafting

The first implication encourages practitioners to be aware of the challenges of InfoSec policy crafting that arise from the likely clash between what are widely accepted prescribed information security practices (i.e., best practices found in, for example, the ISO27001 standard family and the NIST-800 series) and the existing organizational practices. Examples of the clash abound in the publications included in this dissertation. Prior research has further highlighted that when InfoSec policy includes parts that inhibit or slow down employees' work, policy is not turned into actions. In such a case, the clash has not been overcome during crafting, but the policy has remained such that it clashes with the organizational practices. Consequently, overcoming the clash is central for InfoSec policy crafting.

The second implication suggests how practitioners can overcome the clash: best practices and organizational practices should not be directly applied in the policy, but they should be translated before inclusion. That is, policy crafting can begin with generic information security standards, but practitioners should expect to undergo a significant, inclusive effort to adapt these to their organization's strategic, technical, and organizational contexts (i.e., "contextualize" them). Similarly, InfoSec policy crafting should account for the existing organizational practices (i.e., "how things are done here"), but practitioners should not derive the InfoSec policy's practices (i.e., what the policy expects from the firm and its employees) directly from the existing organizational practices. Yet, practitioners should expect some adapted organizational practices to be included in the policy.

The third implication suggests that the practices of borrowing from information security best practices, inviting in-depth participation of various stakeholders, and legitimizing the policy during policy crafting enable the translations from the best practices and organizational practices to the InfoSec policy. *Borrowing practices* means selectively choosing practices (sometimes also called "information security controls") from information security best practices and making changes to them as deemed necessary. The selection and the changes can be made, for example, by considering what is feasible given the organizational reality, resources, and the mandate of those crafting the policy. Information security professionals are likely suitable for enacting this practice. The practice enables the best practices to form the basis of the InfoSec policy. *Inviting in-depth participation* of stakeholders makes these practices fit with the organization. The key to the in-depth participation involves listening to the stakeholders' concerns and providing them with real chances to contribute to policy crafting and to influence what is included in and excluded from the policy. Lip service on the part of the organization's management toward the stakeholders is not an option. By implementing the amendments they suggest, the policy can be made more appropriate. It might even be that a crucial information security practice (from the point of view of information security best practices) is removed from the policy during policy crafting, as the practice of inviting in-depth participation may uncover the infeasibility of the practice in the given context. Specific techniques of inviting participation include workshops and other interactive techniques to gauge stakeholder input to the policy. Inviting participation means that the policy is not made for the organizational members (i.e., "given from above") but with them. *Legitimizing the policy* makes the policy's practices acceptable within the organization and ensures that the policy crafting initiative enjoys legitimacy. Legitimizing entails communicating early, often, and inclusively: practitioners should share why a new policy is needed, describe how the policy crafting process will work and how it is working, demonstrate progress, and celebrate the successful resolution of tough issues. This study further suggests four strategies for legitimizing the policy crafting initiative and the policy itself (see details from publication III):

- Inviting participation
- Embedding into existing practices
- Advertising
- Formalizing and professionalizing

If the policy's practices do not enjoy legitimacy within the organization, the chances are that the policy will not be complied with.

The fourth implication recommends practitioners to recognize that the foundation for InfoSec policy compliance is built already during policy crafting and not only afterwards. Although efforts to promote and achieve compliance often begin after the policy has been crafted, this study suggests that crafting may shape organizational practices towards compliance and that crafting is implicated in policy compliance. In other words, policy crafting can translate the policy's practices into organizational practices. Clearly, if the policy is not turned into actions, policy crafting efforts are in vain.

Figure 6 summarizes the implications as the three pillars of InfoSec policy crafting. It highlights that translating widely accepted information security practices and organizational practices into the organization's InfoSec policy and translating that policy into organizational practice are foundational to any InfoSec policy crafting. These translations are enabled by the practices of (i.e., the three pillars) borrowing from information security best practices, inviting in-depth participation of stakeholders, and legitimizing the policy during policy crafting. Together, the practices build InfoSec policy compliance already during policy crafting.

The implications should not be interpreted as literal prescriptions for successful policy development, but rather as insightful templates for reflection. As a practicing information security professional, I have found these implications valuable beyond the confines of the studied organizations. The publications included in this dissertation provide further implications for practice.

6 CONCLUSION

Information security policy crafting? What crafting? We download those from the Internet! (Chief information security officer from financial sector when I asked for an interview)

Some organizations do not trouble themselves with how their InfoSec policies are developed. This dissertation suggests that they should.

The main argument developed in this dissertation is that researchers and practitioners should not only emphasize the importance of the InfoSec policy or consider its contents and structure or abstract methods of its development, but more emphasis should be on how the policy is crafted. InfoSec policy development does not follow a rote procedure, but is a practical, joined, and skilled accomplishment – a craft. InfoSec policy crafting influences what is included in and excluded from the policy and how the policy will be complied with.

In this concluding chapter, I first summarize the primary contributions of this dissertation. Second, I will note the study's limitations and propose some avenues for future research. Finally, I will provide criteria for evaluating the study's quality.

6.1 Primary contributions

The primary contribution of this dissertation is the conceptualization of InfoSec policy crafting as emerging in the lived contradictions between the international information security best practices (i.e., institutional "rules of the game") and the local organizational practices. The dissertation further suggests that these contradictions are practically and temporarily resolved through translations of the best practices and organizational practices. Practices of InfoSec policy crafting enable the translations. Consequently, InfoSec policy emerges through translations and enabling practices in the policy crafting.

More broadly, this dissertation contributes to research on InfoSec policy development by positing that to understand InfoSec policy crafting requires deep engagement with the actors who participate in the policy crafting and with the field where the policy is crafted. This can be achieved with theories that take ordered constellations of doings and sayings (i.e., practices) seriously and by acknowledging emergence in the crafting. Clearly, it further necessitates research methods that enable the engagement.

Further, this dissertation contributes to discussions around InfoSec policy compliance by suggesting that compliance should not be considered as an afterthought in InfoSec policy development. Rather, compliance should be considered as partly emerging from and through the practices of the policy crafting and as relational to them. The potential for developing the policy as a joint engagement with different organizational members should not be underestimated. Yet, it should be noted that policy compliance materializes in the enactment of that policy in the situated practices. This means that InfoSec policy compliance is a plurality that is relational to the policy crafting.

6.2 Limitations and future research

This research is not without its limitations, which open up avenues for future research. For one thing, the present research has the limits of single case studies and ethnographic studies. This is purposeful as, by design, this study favors depth over statistical generalizability. Thus, it cannot be used for developing statistical generalizations or rule-like statements. On the contrary, by relating the uncovered local ideographic details to broader theoretical ideas, the study aimed to generalize theory (Lee & Baskerville, 2003). Such generalizations differ from statistical generalizations in that they explain situated dynamics in contrast to universal variation. Theoretical generalizations are typical for practice theory-oriented studies in general, where the focus is on the specificities and relational practices (Korica et al., 2017). Therefore, the theoretical generalizations developed through "the use of practice theory are not predictions in the conventional sense but may be better understood as principles that can explain and guide action. They articulate particular relationships or enactments (e.g., technologies in practice, resources in use) that offer insights for understanding other situations while being historically and contextually grounded" (Feldman & Orlikowski, 2011, p. 1249). Yet, although each context of study is different, as "a practice represents a pattern which can be filled out by a multitude of single and often unique actions reproducing the practice" (Reckwitz, 2002b, p. 250), the practices and relationships uncovered and theorized in this study can increase our understanding of InfoSec policy crafting behind the confines of the present study's empirical settings.

Although practices and the concept of translation were central in this study, the present study did not theorize how local, organizational information security practices travel from one context to another, and how those local practices result in field-level changes or become part of "information security best practices." In light of the present study, it would be valuable to understand how the best practices came into being as they seemed central in building the foundation of the studied organizations' InfoSec policies. Previous research has already analyzed the role of power and politics in the setting of information security standards (Backhouse et al., 2006), but new research avenues remain to be explored. Future theorizing should be made with care as the translation approach warns that "all innovations are necessarily 'local', and that the creation and maintenance of uniformities and general standards is something that needs to be explained empirically and not taken for granted" (Nicolini, 2010, p. 1024).

As the purpose of this research is to increase understanding, its limitation is that it tells very little about improving InfoSec policy crafting or how, for example, crafting can be modified to better facilitate InfoSec policy compliance. In this dissertation, participation and legitimization practices in many ways enabled InfoSec policy crafting. These practices invite interaction and open discussion between the organization's management and employees, which encourages the use of more emancipatory policy development methods (Stahl et al., 2011) than top-down enforcement. Therefore, participatory and bottom-up approaches to policy crafting are particularly fruitful avenues for future research. This is especially relevant as the existing research shows that while organizations are increasing aware that a sole top-down approach to policy crafting does not work in contemporary organizations, they struggle to find alternative approaches (Kirlappos et al., 2013). The findings of the present study further suggest that policy crafting and the materiality of the policy have implications for policy compliance. Future research should seek to provide meaningful ways to improve policy crafting. Further, future research on InfoSec policy compliance should take the materiality of the policy and policy crafting more seriously by, for example, incorporating policy crafting into research models.

Although books are the most suitable publication method for ethnographic studies for conveying the richness of the empirical materials and for providing readers with detailed descriptions, journal articles are more highly regarded in information system studies than books (Myers, 1999). Both writing a book and writing articles were not feasible due to the limited resources and time constraints of a doctoral degree. Consequently, I was not able to convey all the details and richness of InfoSec policy crafting I would have wanted to in this dissertation. Writing a book about InfoSec policy crafting would have further enabled a deeper analysis of the reasons why certain practices facilitated the process. This limitation can be overcome in future studies by publishing more detailed stories of InfoSec policy crafting in journal articles such that the issues in the stories become part of a richer story. This would entail rich and detailed descriptions of policy crafting, and how some crafting leads to successful outcomes while others do not. As the present study shows, the practice theory approach is likely relevant for future ethnographic studies in information security management and can offer a firm basis for theorizing and writing up the detailed stories. Practice theories and ethnographic studies may advance our knowledge of information security management phenomena in ways that are both theoretically grounded and which have practical relevance.

6.3 Evaluating the quality of the study

Before concluding, it is worth considering some of the quality-related aspects of the present research. Different qualitative research approaches have different evaluation criteria associated with them (Sarker et al., 2013). That is, they cannot be evaluated by a single (positivist) criteria of reliability and validity (ibid.). Different criteria for evaluating the quality of ethnographic and case studies exists (e.g., Golden-Biddle & Locke, 1993; Locke & Golden-Biddle, 1997; Klein & Myers, 1999; Myers, 1999). Yet, neither ethnography nor case study can be evaluated by a pre-determined criteria that is applied mechanistically (Klein & Myers, 1999), but researchers should lay out the criteria through which they think their research should be assessed (Davidson, 2002). In the following, I reflect on the quality of the study by discussing this research in light of Myers' (1999) four requirements: "(a) contribution (novelty and capacity to convince the journal editorial board of this), (b) rich insights (one way to address this being to consider whether it contradicts conventional wisdom), (c) significant amount of data collected (involvement of the researcher on the field to get data; contextualization, multiple stakeholders perspectives), (d) sufficient description of the method" (Rowe, 2012, p. 474).

The first requirement relates to a study's contribution and in particular to convincing "the reviewers and editors who serve on the editorial boards of our journals" that the findings are new (Myers, 1999, pp. 11–12). All publications included in this dissertation are published in acclaimed journals, well-established conferences, or books; thus, the reviewers and editors have arguably found the findings worth publishing. I have further discussed the contributions of this study in Chapter 5, "Discussion" and related them to the existing research. By doing so, I have sought to relate the present research to the established knowledge in the information security field and connected the findings to broader literature to establish plausibility of the contributions (Golden-Biddle & Locke, 1993).

The second requirement is about providing readers with rich insights that sometimes even contradict the conventional thinking. The present study illustrates that separating InfoSec policy development, implementation, and compliance, as is typically done in information security research, may be an inappropriate conceptualization. Describing how policy comes into being as a set of phases that flow linearly or as a "formulation" may also imply misleading connotations. Rather, development, implementation, and compliance mingle in InfoSec policy crafting. The central role of participation may further be against some readers' expectations and assumptions, as traditional information security research has not properly taken advantage of organizational members' knowledge (Siponen, 2005). Such findings seek to illustrate the criticality (Golden-Biddle & Locke, 1993) employed in the research process.

The third requirement is about the amount of empirical material collected during the research process. For ethnographic research, this requirement relates particularly to empirical material collected through participant observation (Myers, 1999). For both ethnographic studies, I spent considerable time (i.e., six and 15 months) at the studied organizations and was involved in the research settings through workshops, meetings, and informal occasions. I engaged with organizational members' work lives, watched what happened, listened to what was said, and asked questions. I did not only listen to the "official line" promoted by the organizations' management or information security professionals, but sought to uncover what was behind the official facade. For example, this is shown in the description of the InfoSec policy crafting in publication I that illustrates various contradictions between the organization's management, the information security professionals, and the employees.

The fourth requirement is about providing readers with sufficient information about the research methods used. In essence, "[a]nyone reading the published article should be able to evaluate for themselves the 'validity' of the findings" (Myers, 1999, pp. 12–13). I have sought to openly describe the research process and my rationale for selecting my particular research methods in order to provide readers with enough information to evaluate the "validity" of the findings. I have done this both in the publications and in Chapter 3, "Research approach." I have further provided information about my background and my role as the researcher in each study in Section 3.3.4, "Access to the research settings and the researcher's role."

REFERENCES

Adams, A. & Blandford, A. 2005, 'Bridging the gap between organizational and user perspectives of security in the clinical domain', *International Journal of Human-Computer Studies*, vol. 63, no. 1-2, pp. 175-202.

Almklov, P. G. & Antonsen, S. 2014 'Making work invisible: New public management and operational work in critical infrastructure sectors', *Public Administration*, vol. 92, no. 2, pp. 477-492.

Alvesson, M. 2003, 'Beyond neopositivists, romantics, and localists: A reflexive approach to interviews in organizational research', *Academy of Management Review*, vol. 28, no. 1, pp. 13-33.

Backhouse, J., Hsu, C. W. & Silva, L. 2006, 'Circuits of power in creating de jure standards: Shaping an international information systems security standard', *MIS Quarterly*, vol. 30, no. Special Issue, pp. 413-438.

Barad, K. 2003, 'Posthumanist performativity: Toward an understanding of how matter comes to matter', *Signs: Journal of Women in Culture and Society*, vol. 28, no. 3, pp. 801-831.

Barad, K. 2007, *Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning*, Duke University Press, London, UK.

Barnes, B. 2001, 'Practice as collective action', in T. R. Schatzki, K. K. Cetina & E. von Savigny (eds.), *The Practice Turn in Contemporary Theory*, Routledge, London, UK.

Baskerville, R. & Siponen, M. 2002, 'An information security meta-policy for emergent organizations', *Logistics Information Management*, vol. 15, no. 5/6, pp. 337-346.

Baskerville, R. L. & Dhillon, G. 2008, 'Information systems security strategy: A process view', in D. W. Straub, S. Goodman & R. L. Baskerville (eds.), *Information Security: Policy, Processes and Practices*, M.E. Sharpe, Armonk, NY.

Björck, Fredrik, J. (2005). *Discovering Information Security Management*. Unpublished dissertation, Stockholm University & Royal Institute of Technology.

Bourdieu, P. 1990, *The Logic of Practice*, Polity Press, Cambridge, UK.

Bromley, P. & Powell, W. W. 2012, 'From smoke and mirrors to walking the talk: Decoupling in the contemporary world', *Academy of Management Annals*, vol. 6, no. 1, pp. 483-530.

Brown, J. S. & Duguid, P. 1991, 'Organizational learning and communities-of-practice: Toward a unified view of working, learning, and innovation', *Organization Science*, vol. 2, no. 1, pp. 40-57.

National Institute of Standards and Technology 2006, *NIST Special Publication 800-100: Information Security Handbook: A Guide for Managers: Information Security*.

Ciborra, C. U. 1997, 'De profundis? Deconstructing the concept of strategic alignment', *Scandinavian Journal of Information Systems*, vol. 9, no. 1, pp. 67-82.

Corpuz, M. & Barnes, P. H. 2010, 'Integrating information security policy management with corporate risk management for strategic alignment', *Proceedings of the 14th World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2010)*, pp. 1-7.

Czarniawska, B. & Joerges, B. 1996, 'Travels of ideas', in B. Czarniawska & G. Sevón (eds.), *Translating Organizational Change*, Walter de Gruyter, Berlin, DE.

Dhillon, G. & Torkzadeh, G. 2006, 'Value-focused assessment of information system security in organizations', *Information Systems Journal*, vol. 16, no. 3, pp. 293-314.

Dhillon, G. 2007, *Principles of Information Systems Security: Text and Cases*, John Wiley & Sons, Inc., Hoboken, NJ.

Dick, P. 2015, 'From rational myth to self-fulfilling prophecy? Understanding the persistence of means–ends decoupling as a consequence of the latent functions of policy enactment', *Organization studies*, vol. 36, no. 7, pp. 897-924.

Doherty, N. F., Anastasakis, L. & Fulford, H. 2009, 'The information security policy unpacked: A critical study of the content of university policies', *International Journal of Information Management*, vol. 29, no. 6, pp. 449-457.

Doherty, N. F. & Fulford, H. 2006, 'Aligning the information security policy with the strategic information systems plan', *Computers & Security*, vol. 25, no. 1, pp. 55-63.

Eloff, J. & Eloff, M. 2005, 'Information security architecture', *Computer Fraud & Security*, vol. 2005, no. 11, pp. 10-16.

Feldman, M. S. 2000, 'Organizational routines as a source of continuous change', *Organization Science*, vol. 11, no. 6, pp. 611-629.

Feldman, M. S. & Orlikowski, W. J. 2011, 'Theorizing practice and practicing theory', *Organization Science*, vol. 22, no. 5, pp. 1240-1253.

Ferreira, A., Antunes, L., Chadwick, D. & Correia, R. 2010, 'Grounding information security in healthcare ', *International Journal of Medical Informatics*, vol. 79, no. 4, pp. 268-283.

Flowerday, S. V. & Tuyikeze, T. 2016, 'Information security policy development and implementation: The what, how and who', *Computers & Security*, vol. 61, pp. 169-183.

Fulford, H. & Doherty, N. F. 2003, 'The application of information security policies in large UK-based organizations: an exploratory investigation', *Information Management & Computer Security*, vol. 11, no. 3, pp. 106-114.

Gherardi, S. 2009, 'Introduction: The critical power of the 'practice lens'', *Management Learning*, vol. 40, no. 2, pp. 115-128.

Goel, S. & Chengalur-Smith, I. N. 2010, 'Metrics for characterizing the form of security policies', *The Journal of Strategic Information Systems*, vol. 19, no. 4, pp. 281-295.

Golden-Biddle, K. & Locke, K. 1993, 'Appealing work: An investigation of how ethnographic texts convince', *Organization Science*, vol. 4, no. 4, pp. 595-616.

Halinen, A. & Törnroos, J.-Å. 2005, 'Using case methods in the study of contemporary business networks', *Journal of Business Research*, vol. 58, pp. 1258-1297.

Hannerz, U. 2003, 'Being there... and there... and there! Reflections on multi-site ethnography', *Ethnography*, vol. 4, no. 2, pp. 201–16.

Hedström, K., Kolkowska, E., Karlsson, F. & Allen, J. P. 2011, 'Value conflicts for information security management', *Journal of Strategic Information Systems*, vol. 20, no. 4, pp. 373-384.

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, pp. 106-125.

Höne, K. & Eloff, J. H. P. 2002a, 'What makes an effective information security policy?', *Network Security*, vol. 2002, no. 6, pp. 14-16.

Höne, K. & Eloff, J. H. P. 2002b, 'Information security policy - What do international information security standards say?', *Computers & Security*, vol. 21, no. 5, pp. 402-409.

Hong, K.-S., Chi, Y.-P., Chao, L. R. & Tang, J.-H. 2006, 'An empirical study of information security policy on information security elevation in Taiwan', *Information Management and Computer Security*, vol. 14, no. 2, pp. 104-115.

Hsu, C. W. 2009, 'Frame misalignment: interpreting the implementation of information systems security certification in an organization', *European Journal of Information Systems*, vol. 18, no. 2, pp. 140-150.

Hsu, C., Lee, J.-N. & Straub, D. W. 2012, 'Institutional influences on information systems security innovations', *Information Systems Research*, vol. 23, no. 3-Part-2, pp. 918-939.

Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., & Lowry, P. B. 2015, 'The role of extra-role behaviors and social controls in information security policy effectiveness', *Information systems research*, vol. 26, no. 2, pp. 282-300.

Ifinedo, P. 2014, 'Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition', *Information & Management*, vol. 51, no. 1, pp. 69-79.

Inglesant, P. & Sasse, M. A. 2011, 'Information security as organizational power: A framework for re-thinking security policies', *2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, pp. 9-16.

ISO/IEC 2013a, *ISO/IEC 27001: Information Technology - Security Techniques - Information Security Management Systems - Requirements*.

ISO/IEC 2013b, *ISO/IEC 27002: Information Technology - Security Techniques - Code of Practice for Information Security Controls*.

ISO/IEC 2014, *ISO/IEC 27000: Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary*.

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.

Jarzabkowski, P. A., Le, J. K. & Feldman, M. S. 2012, 'Toward a theory of coordinating: Creating coordinating mechanisms in practice', *Organization Science*, vol. 23, no. 4, pp. 907-927.

Jick, T. D. 1979, 'Mixing qualitative and quantitative methods: Triangulation in action', *Administrative Science Quarterly*, vol. 24, no. 4, pp. 602-611.

Johnston, A. C., Warkentin, M. & Siponen, M. 2015, 'An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric'. *MIS Quarterly*, vol. 39, no. 1, pp. 113-134.

Johnston, A. C., Warkentin, M., McBride, M. & Carter, L. 2016, 'Dispositional and situational factors: influences on information security policy violations', *European Journal of Information Systems*, vol. 25, no. 3, pp. 231-251.

Kaplan, S. 2007, 'Reviewed work: Strategy as practice: An activity-based approach by Paula Jarzabkowski', *The Academy of Management Review*, vol. 32, no. 3, pp. 986-990.

Kappelman, L., Johnson, V., McLean, E. & Torres, R. 2016, 'The 2015 SIM IT issues and trends study', *MIS Quarterly Executive*, vol. 15, no. 1, pp. 55-83.

Karlsson, F., Hedström, K. & Goldkuhl, G. 2017, 'Practice-based discourse analysis of information security policies', *Computers & Security*, vol. 67, pp. 267-279.

Karyda, M., Kiountouzis, E. & Kokolakis, S. 2005, 'Information systems security policies: a contextual perspective', *Computers & Security*, vol. 24, no. 3, pp. 246-260.

Klein, H. K. & Myers, M. D. 1999, 'A set of principles for conducting and evaluating interpretive field studies in information systems', *MIS Quarterly*, vol. 23, no. 1, pp. 67-93.

Klein, H. K. & Rowe, F. 2008, 'Marshaling the professional experience of doctoral students: A contribution to the practical relevance debate', *MIS Quarterly*, vol. 32, no. 4, pp. 675-686.

Kirlappos, I., Beutement, A. & Sasse, M. A. 2013, '"Comply or die" is dead: Long live security-aware principal agents', in A. A. Adams, M. Brenner & M. Smith (eds.), *Financial Cryptography and Data Security: FC 2013 Workshops, USEC and WAHC 2013, Okinawa, Japan, April 1, 2013, Revised Selected Papers*, Springer Berlin / Heidelberg.

Knapp, K. J., Morris, R. F. J., Marshall, T. E. & Byrd, T. A. 2009, 'Information security policy: An organizational-level process model', *Computers& Security*, vol. 28, no. 7, pp. 493-508.

Kolkowska, E. & Dhillon, G. 2013, 'Organizational power and information security rule compliance', *Computers & Security* , vol. 33, no. 0, pp. 3-11.

Kolkowska, E., Karlsson, F. & Hedström, K. 2017, 'Towards analysing the rationale of information security non-compliance: Devising a value-based compliance analysis method', *Journal of Strategic Information Systems*, vol. 26, no. 1, pp. 39-57.

Korica, M., Nicolini, D. & Johnson, B. 2017, 'In search of 'managerial work': Past, present and future of an analytical category', *International Journal of Management Reviews*, vol. 19, no. 2, pp. 151-174.

Kvale, S. 1996, *InterViews: An Introduction to Qualitative Research Interviewing*, Sage Publications, Thousand Oaks, California.

Kvale, S. & Brinkmann, S. 2009, *InterViews: Learning the Craft of Qualitative Research Interviewing Second Edition*, SAGE Publications, Inc, Thousand Oaks, California.

Langley, A. 1999, 'Strategies for theorizing from process data', *The Academy of Management Review*, vol. 24, no. 4, pp. pp. 691-710.

Lapke, M. & Dhillon, G. 2008, 'Power relationships in information systems security policy formulation and implementation', *ECIS 2008 Proceedings*.

Lapke, M. S. (2008). *Power Relationships in Information Systems Security Policy Formulation and Implementation*. Unpublished dissertation, Virginia Commonwealth University, Richmond, Virginia.

Lee, A. S. & Baskerville, R. L. 2003, 'Generalizing generalizability in information systems research', *Information Systems Research*, vol. 14, no. 3, pp. 221-243.

Levina, N. & Vaast, E. 2005, 'The emergence of boundary spanning competence in practice: Implications for implementation and use of information systems', *MIS Quarterly*, vol. 29, no. 2, pp. 335-363.

Lincoln, Y. S. & Guba, E. G. 1985, *Naturalistic Inquiry*, SAGE Publications, Inc, Beverly Hills, CA.

Locke, K. & Golden-Biddle, K. 1997 'Constructing opportunities for contribution: Structuring intertextual coherence and "problematizing" in organizational studies', *The Academy of Management Journal*, vol. 40, no. 5, pp. 1023-1062.

Lounsbury, M. & Crumley, E. T. 2007, 'New practice creation: An institutional perspective on innovation', *Organization Studies*, vol. 28, no. 7, pp. 993-1012.

Lowry, P. B. & Moody, G. D. 2015, 'Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies', *Information Systems Journal*, vol. 25, no. 5, pp. 433-463.

Ma, Q., Johnston, A. C. & Pearson, J. M. 2008, 'Information security management objectives and practices: a parsimonious framework', *Information Management & Computer Security*, vol. 16, no. 3, pp. 251-270.

van Maanen, J. 2011, 'Ethnography as work: some rules of engagement', *Journal of Management Studies*, vol. 48, no. 1, pp. 218-234.

Marcus, G., 1995, 'Ethnography in/of the world system: The emergence of multi-sited ethnography', *Annual Review of Anthropology*, vol. 24, pp. 95–117.

Merriam-Webster (2017). Merriam-Webster dictionary. Available at: https://www.merriam-webster.com/dictionary/craft (accessed 14 April 2017).

Miettinen, R., Samra-Fredericks, D. & Yanow, D. 2009, 'Re-turn to practice: An introductory essay', *Organization Studies*, vol. 30, no. 12, pp. 1309-1327.

Miles, M. B. & Huberman, A. M. 1994, *Qualitative Data Analysis: An Expanded Sourcebook*, SAGE Publications, Inc, Thousand Oaks, CA.

Mintzberg, H. 1987, 'Crafting strategy', *Harvard Business Review*, vol. 65, no. 4, pp. 66-75.

Myers, M. 1999, 'Investigating information systems with ethnographic research', *Communications of the AIS*, vol. 2, no. 4es, pp. 1.

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, pp. 126-139.

Nasution, F. M. & Dhillon, G. 2012, 'Shaping of security policy in an Indonesian bank: Interpreting institutionalization and structuration', *ECIS 2012 Proceedings*.

Nicolini, D. 2009a, 'Zooming in and out: Studying practices by switching theoretical lenses and trailing connections', *Organization Studies*, vol. 30, no. 12, pp. 1391-1418.

Nicolini, D. 2009b, '6 Zooming in and zooming out: A package of method and theory to study work practices', in S. Ybema, D. Yanow, H. Wels & F. Kamsteeg (eds.), *Organizational Ethnography: Studying the Complexities of Everyday Life*, SAGE Publications Ltd, London, UK.

Nicolini, D. 2012, *Practice Theory, Work, and Organization*, Oxford University Press, Oxford.

Niemimaa, M., Laaksonen, E. & Harnesk, D. 2013, 'Interpreting information security policy outcomes: A frames of reference perspective', *46th Hawaii International Conference on System Sciences*, pp. 4541-4550.

Njenga, K. & Brown, I. 2012, 'Conceptualising improvisation in information systems security', *European journal of information systems*, vol. 21, pp. 592-607.

Orlikowski, W. J. 1991, 'Integrated information environment or matrix of control? The contradictory implications of information technology', *Accounting, Management and Information Technologies*, vol. 1, no. 1, pp. 9-42.

Orlikowski, W. J. & Baroudi, J. J. 1991, 'Studying information technology in organizations: Research approaches and assumptions', *Information Systems Research*, vol. 2, no. 1, pp. 1-28.

Orlikowski, W. J. 2000, 'Using technology and constituting structures: A practice lens for studying technology in organizations', *Organization Science*, vol. 11, no. 4, pp. 404-428.

Orlikowski, W. J. 2002, 'Knowing in practice: Enacting a collective capability in distributed organizing', *Organization Science*, vol. 13, no. 3, pp. 249-273.

Orr, J. E. 1996, *Talking About Machines: An Ethnography of Modern Work*, ILR Press/Cornell University Press, US.

Orr, J. E. 1998, 'Images of work', *Science Technology Human Values*, vol. 23, no. 4, pp. 439-455.

Palmer, M. E., Robinson, C., Patilla, J. C. & Moser, E. P. 2001, 'Information security policy framework: Best practices for security policy in the E-commerce age', *Information Systems Security*, vol. 10, no. 2, pp. 13-27.

Ponemon Institute LLC 2013, *Is Your Company Ready for a Big Data Breach?*.

Ponemon Institute LLC. 2015, *2015 Cost of Data Breach Study: Global Analysis*.

Reckwitz, A. S. 2002a, 'Toward a theory of social practices: A development in culturalist theorizing'. *European journal of social theory*, vol. 5, no. 2, pp. 243-263.

Reckwitz, A. S. 2002b, 'The status of the "material" in theories of culture: From "social structure" to "artefacts"', *Journal for the theory of social behaviour*, vol. 32, no. 2, pp. 195-217.

Rees, J., Bandyopadhyay, S. & Spafford, E. H. 2003, 'PFIRES: A policy framework for information security', *Communications of the ACM*, vol. 46, no. 7, pp. 101-106.

Rowe, F. 2012, 'Toward a richer diversity of genres in information systems research: new categorization and guidelines', *European Journal of Information Systems*, vol. 21, no. 5, pp. 469-487.

Sahlin, K. & Wedlin, L. 2008, 'Circulating ideas: Imitation, translation and editing', in R. Greenwood, C. Oliver, K. Sahlin & R. Suddaby (eds.), *The Sage Handbook of Organizational Institutionalism*, SAGE: London, London, UK.

Saint-Germain, R. 2005, 'Information security management best practice based on ISO/IEC 17799', *Information Management Journal*, vol. 39, no. 4, pp. 60-66.

Sandberg, J. & Tsoukas, H. 2011, 'Grasping the logic of Practice: Theorizing through practical rationality', *Academy of Management Review*, vol. 36, no. 2, pp. 338-360.

Sarker, S., Xiao, X & Beulieu, T. 2013, 'Qualitative studies in information systems: A critical review and some guiding principles', *MIS Quarterly*, vol. 37, no. 4, pp. iii - xviii.

Schatzki, T. R. 2001, 'Introduction', in T. R. Schatzki, K. K. Cetina & E. von Savigny (eds.), *The Practice Turn in Contemporary Theory*, Routledge, London, UK.

Schatzki, T.R., Cetina, K. K. & von Savigny, E. (eds.) 2001, *The Practice Turn in Contemporary Theory*, Routledge, London, UK.

Schatzki, T. R. 2002, *The Site of the Social: A Philosophical Account of the Constitution of Social Life and Change*, The Pennsylvania State University Press, University Park, US.

Schatzki, T. R. 2005, 'The sites of organizations', *Organization Studies*, vol. 26, no. 3, pp. 465-484.

Schultze, U. 2000, 'A confessional account of an ethnography about knowledge work', *MIS quarterly*, vol. 24, no. 1, pp. 3-41.

Schultze, U. & Orlikowski, W. J. 2004, 'A practice perspective on technology-mediated network relations: The use of internet-based self-serve technologies', *Information Systems Research*, vol. 15, no. 1, pp. 87-106.

Sevón, G. 1996, 'Organizational imitation in identity transformation', in B. Czarniawska & G. Sevón (eds.), *Translating Organizational Change*, Walter de Gruyter, Berlin, New York.

Siggelkow, N. 2007, 'Persuasion with case studies', *Academy of Management Journal*, vol. 50, no.1, pp. 20-24.

Siponen, M. 2005b, 'An analysis of the traditional IS security approaches: Implications for research and practice', *European Journal of Information Systems*, vol. 14, pp. 303-315.

Siponen, M. 2005a, 'Analysis of modern IS security development approaches', *Information and Organization*, vol. 15, no. 4, pp. 339-375.

Siponen, M. 2006, 'Information security standards focus on the existence of process, not its content', *Communications of the ACM*, vol. 49, no. 8, pp. 97-100.

Siponen, M. & Iivari, J. 2006, 'Six design theories for IS security policies and guidelines', *Journal of the Association for Information Systems*, vol. 7, no. 7, pp. 445-472.

Siponen, M., Willison, R. & Baskerville, R. 2008, 'Power and practice in information systems security research', *ICIS 2008 Proceedings*.

Siponen, M., Pahnila, S. & Mahmood, M. 2010, 'Compliance with information security policies: An empirical investigation', *IEEE Computer Society*, vol. 43, no. 2, pp. 64 -71.

Siponen, M. T. & Oinas-Kukkonen, H. 2007, 'A review of information security issues and respective research contributions', *SIGMIS Database*, vol. 38, no. 1, pp. 60-80.

Smets, M., Morris, T. & Greenwood, R. 2012, 'From practice to field: A multilevel model of practice-driven institutional change', *Academy of Management Journal*, vol. 55, no. 4, pp. 877-904.

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.

von Solms, R. 1999, 'Information security management: why standards are important', *Information Management & Computer Security*, vol. 7, no. 1, pp. 50-57.

von Solms, B. 2005, 'Information security governance: COBIT or ISO 17799 or both?', *Computers & Security*, vol. 24, pp. 99-104.

Spears, J. L. & Barki, H. 2010, 'User Participation in information systems security risk management', *MIS Quarterly*, vol. 34, no. 3, pp. 503-A5.

Stahl, B. C., Tremblay, M. C. & LeRouge, C. M. 2011, 'Focus groups and critical social IS research: How the choice of method can promote emancipation of respondents and researchers', *European Journal of Information Systems*, vol. 20, no. 4, pp. 378-394.

Stahl, B., Doherty, N. & Shaw, M. 2012, 'Information security policies in the UK healthcare sector: A critical evaluation', *Information Systems Journal*, vol. 22, no. 1, pp. 77-94.

Straub, D. W., Goodman, S. & Baskerville, R. L. 2008, 'Framing the information security process in modern society', in D. W. Straub, S. Goodman & R. L. Baskerville (eds.), *Information Security: Policy, Processes and Practices*, M.E. Sharpe, Armonk, NY.

Straub, D. W. & Welke, R. J. 1998, 'Coping with systems risk: Security planning models for management decision making', *MIS Quarterly*, vol. 22, no. 4, pp. pp. 441-469.

Suchman, L. A. 2007, *Human-Machine Reconfigurations: Plans and Situated Actions*, Cambridge University Press, Lancaster University, UK.

Trcek, D. 2003, 'An integral framework for information systems security management', *Computers & Security*, vol. 22, no. 4, pp. 337-360.

Trompeter, C. & Eloff, J. H. P. 2001, 'Framework for the implementation of socio-ethical controls in information security', *Computers & Security*, vol. 20, no. 5, pp. 384-391.

Tsohou, A., Karyda, M., Kokolakis, S. & Kiountouzis, E. 2012, 'Analyzing trajectories of information security awareness', *Information Technology & People*, vol. 25, no. 3, pp. 327-352.

Tsoukas, H. & Chia, R. 2002, 'On organizational becoming: Rethinking organizational change', *Organization Science*, vol. 13, no. 5, pp. 567-582.

Vaara, E. & Whittington, R. 2012, 'Strategy-as-practice: taking social practices seriously', *The Academy of Management Annals*, vol. 6, no. 1, pp. 285-336.

Vance, A., Siponen, M. & Pahnila, S. 2012, 'Motivating IS security compliance: Insights from habit and protection motivation theory', *Information & Management*, vol. 49, pp. 190-198.

Warkentin, M. & Johnston, A. C. 2008, 'IT governance and organizational design for security management', in D. W. Straub, S. E. Goodman & R. Baskerville (eds.), *Information Security: Policy, Processes and Practices*, M.E. Sharpe, Armonk, NY.

Warkentin, M. & Willison, R. 2009, 'Behavior and policy issues in information systems security: The insider threat', *European Journal of Information Systems*, vol. 18, pp. 101-105.

Whitman, M. E. 2008, 'Security policy: From design to maintenance', in D. W. Straub, S. Goodman & R. L. Baskerville (eds.), *Information Security: Policy, Processes and Practices*, M.E. Sharpe, Armonk, NY.

Whitman, M. E. 2004, 'In defense of the realm: understanding the threats to information security', *International Journal of Information Management*, vol. 24, no. 1, pp. 43-57.

Whittington, R. 2006, 'Completing the practice turn in strategy research', *Organization Studies*, vol. 27, no. 5, pp. 613-634.

Yin, R. K. 1989, *Case Study Research: Design and Methods*, 2nd edition, Sage Publications, Inc., Thousand Oaks.

APPENDIX A: OBSERVATION NOTES TEMPLATE AND EXCERPT FROM OBSERVATION NOTES

Table 7 includes an excerpt from my observation notes. I adopted the observation note template from Schultze (2000, p. 17). I have translated the parts of the text that were originally in Finnish and removed the date from the observation note excerpt.

Table 7: Excerpt from observation notes

Date:
Location: headquarters
Main events: a workshop to review policy draft's information security practices related to project methodology
Small/Odd events:
Main players: chief financial officer (CFO), chief information security officer (CISO), external consultant
Detailed description of the day (pick the main events and describe): The CFO was about 15 minutes late from the workshop. The CISO and the consultant thought that perhaps he will not appear at all and began to do some other work. Suddenly, the CFO appeared at the workshop and expressed his apologies for being late. He explained that he had been talking with the chief information officer (CIO). Without sitting down and before the CISO had a chance to say anything, the CFO was urged to explain that he understood that "this information security is a very important topic and of course it must be included in the methodology," but he also emphasized that the new project methodology must be light, as lean as possible, and nothing excessive can be included. He continued (still standing) that he can show the methodology and displayed it on a screen. He again mentioned that it was very important that the new methodology be light and explained that compliance to the methodology will be monitored by quality function. The CISO and consultant seemed dazed and barely nodded. They had no chance to say anything as the CFO continued to speak as if he were on fire. Suddenly, the CFO stopped talking by saying: "I think this information security can have at most two checkpoints in the project methodology. One at the beginning and one at the end. Nothing more. I clearly see that this is important but two is enough." Then he turned to the CISO as if asking: "Understood? Two is enough." [...]
Early interpretation/Personal notes: The CFO talking about the importance of information security seems to me that he is merely playing lip service. The CISO and the consultant have no chance to challenge the CFO. What will the CISO and the consultant do now? They had planned to include several information security practices in the methodology. Will they remove them from the policy draft?

APPENDIX B: PUBLICATIONS

Publication I: Information systems security policy implementation in practice: from best practices to situated practices

Niemimaa, E. & Niemimaa, M. 2017, 'Information systems security policy implementation in practice: from best practices to situated practices', European Journal of Information Systems, vol. 25, no. 1, pp. 1–20.

Publication II: Crafting an information security policy: insights from an ethnographic study

Niemimaa, E. 2016, ‘Crafting an information security policy: insights from an ethnographic study’, Proceedings of the 37th International Conference on Information Systems (ICIS 2016), pp. 1–16.

Publication III: Legitimising information security policy during policy crafting: exploring legimitising strategies

Niemimaa, E. 2016, ‘Legitimising information security policy during policy crafting: exploring legimitising strategies’, Proceedings of the 27th Australian Conference on Information Systems (ACIS 2016), pp. 1-11.

Publication IV: A practice lens for understanding the organizational and social challenges of information security management

Niemimaa, E. 2016, ‘A practice lens for understanding the organizational and social challenges of information security management’, Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS 2016), paper 58.

Publication V: Enacting information security policies in practice: three modes of policy compliance

Niemimaa, M. & Laaksonen, A. E. 2015, ‘Enacting information security policies in practice: three modes of policy compliance’, in F.-X. de Vaujany, N. Mitev, G. F. Lanzara, & A. Mukherjee (eds.), Materiality, Rules and Regulation: New Trends in Management and Organization Studies, Palgrave Macmillan.

Tampereen teknillinen yliopisto
PL 527
33101 Tampere

Tampere University of Technology
P.O.B. 527
FI-33101 Tampere, Finland

ISBN 978-952-15-4037-0
ISSN 1459-2045