Digital Transformation and IT Security Issues

Analyzing Organizational Decision-Making Processes through a Behavioral Lens

TECHNISCHE UNIVERSITÄT DARMSTADT

Vom Fachbereich Rechts- und Wirtschaftswissenschaften
der Technischen Universität Darmstadt

genehmigte

Dissertation

von

Margareta Heidt M.Sc.
geboren am 11.12.1988 in Tschirtschik (Usbekistan)

zur Erlangung des akademischen Grades
Doctor rerum politicarum (Dr. rer. pol.)

Erstgutachter:	Prof. Dr. Peter Buxmann
Zweitgutachter:	Prof. Dr. Alexander Benlian
Hochschulkennziffer:	D17
Darmstadt	2020

Heidt, Margareta: Digital Transformation and IT Security Issues - Analyzing Organizational Decision-Making Processes through a Behavioral Lens

Darmstadt, Technische Universität Darmstadt

Veröffentlichungsjahr der Dissertation auf TUprints im Jahr 2021

URN: urn:nbn:de:tuda-tuprints-189016
Tag der mündlichen Prüfung: 14.06.2021

Declaration of Authorship

I hereby declare that the submitted thesis is my own work. All quotes, whether word by word or in my own words, have been marked as such.

The thesis has not been published anywhere else nor presented to any other examination board.

Ich erkläre hiermit ehrenwörtlich, dass ich die vorliegende Arbeit selbstständig angefertigt habe. Sämtliche aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht.

Die Arbeit wurde bisher weder einer anderen Prüfungsbehörde vorgelegt noch veröffentlicht.

Margareta Heidt

Darmstadt, 18.09.2020

Abstract

Digital transformation has established itself as an omnipresent term in the new millennium. Often considered synonymous with the so-called Fourth Industrial Revolution, the term describes the convergence of information technology and the ubiquity of data in private life as well as in business and social lives. Inherent to the term "revolution" is radical change and the upheaval of existing processes and relationships. Translated into a business context, revolution leads to the transformation of business models and established work processes as well as the increasing dependence on data and new technologies. In times of digital transformation, managers and organizational decision-makers are faced with constant, potentially business-critical, decisions regarding these new technologies and the maintenance of information and data security. The analysis of management decisions, therefore, plays a crucial role in comprehending and researching digital transformation.

This dissertation, therefore, seeks to improve our understanding of decision-making processes regarding the adoption of cloud computing solutions and data protection measures as well as investments in information technology (IT) security in primarily small and medium-sized enterprises.

Article A examines the influence of status quo bias and reference dependency in the decision to adopt cloud computing solutions. Based on the tenets of prospect theory, findings suggest that rather inexperienced decision-makers are taking their evaluation of the existing technology more into account when assessing a cloud-based replacement technology. As a consequence, status quo thinking leads to a more negative assessment of the new technology, which hinders its potentially beneficial introduction to the organizational IT service architecture.

Article B investigates decision-making processes related to end-user data protection measures and the impact of psychological ownership on the motivation to protect data. In a questionnaire study and based on the protection motivation theory, the influence of psychological ownership on the decision-making behavior of individuals in both private and work contexts is analyzed. The results demonstrate that psychological ownership exerts a stronger impact on the protection motivation of participants in a private context. The analysis further indicates that employees

partly relinquish their responsibility regarding security responses to protect data in their work context. Fostering feelings of psychological ownership could possibly counteract such detrimental effects and improve the adoption of data protection measures in a work context.

In Article C, the previously demonstrated cognitive and behavioral aspects of decision-making are contextualized into a holistic conceptual framework. Based on a comprehensive literature analysis and an interview study, this study finds that decisions regarding IT security in companies are influenced by organizational, economic, environmental, cognitive, and behavioral aspects. The literature analysis further demonstrates that existing research still emphasizes economic aspects based on the assumption of purely rational decision-makers. Studies that shed light on IT security decisions from a behavioral, environmental or organizational perspective are significantly less frequent, although the analysis of the expert interviews emphasizes the influence of these aspects.

Article D validates that decision-makers in companies are influenced by a variety of aspects when making investment decisions in IT security. The studies of both Article D and Article E aim at decision-makers from small and medium-sized enterprises (SMEs), since an in-depth literature review of existing research in the area of organizational IT security indicates that organizational IT security in SMEs has been largely neglected. The analysis of expert interviews conducted with SME decision-makers, however, indicates that implications of existing research can be transferred only to a limited extent due to unique constraints and their influence on decisions in the SME context. The studies, therefore, investigate and validate the impact of these SME-specific constraints regarding IT security decisions. The findings imply that investment decisions with regard to organizational IT security are strongly influenced by SME-specific characteristics such as insufficient IT budget planning, undocumented processes, or multiple roles due to lack of resources.

Consequently, this dissertation provides valuable insights for both practice and research regarding typical and frequent decision-making processes in the context of digital transformation. In particular, this study examines the influence of biases and non-rational aspects in the decision-making process regarding new technologies or measures to ensure their security as well as the effects of SME-specific constraints demonstrate and emphasizes the need for further behavioral research in technology adoption and IT security.

Abstract (Deutsche Übersetzung)

Digitale Transformation hat sich als omnipräsenter Begriff im neuen Jahrtausend etabliert. Oft gleichbedeutend mit der sogenannten Vierten Industriellen Revolution, beschreibt der Begriff die Konvergenz von Informationstechnologie und die Allgegenwärtigkeit von Daten im privaten, geschäftlichen und gesellschaftlichen Kontext. Der „Revolution“ inne ist die radikale Veränderung und Umwälzung bestehender Verhältnisse und Prozesse. Für die Wirtschaft führt dies einerseits zur Wandlung von Geschäftsmodellen und etablierten Arbeitsprozessen sowie andererseits zu einer steigenden Abhängigkeit von Daten und neuen Technologien. Führungskräfte und Entscheidungsträger müssen in Zeiten Digitaler Transformation und der damit einhergehenden Komplexität, fortlaufend potenziell geschäftskritische Entscheidungen treffen. Die Analyse von Managemententscheidungen nimmt damit eine zentrale Rolle für das Verständnis und die Forschung bezüglich Digitaler Transformation ein.

Diese Dissertation widmet sich deswegen Entscheidungsprozessen hinsichtlich diverser Initiativen im Rahmen einer Digitalen Transformationsstrategie. Diese Initiativen umfassen konkret die Adoption von Cloud Computing-Lösungen und Datenschutzmaßnahmen sowie Investitionsentscheidungen in IT-Sicherheit im Kontext vornehmlich kleiner und mittelgroßer Unternehmen.

Artikel A beleuchtet dabei den Einfluss des sogenannten Status Quo Bias und der Referenzabhängigkeit bei Ablöseentscheidungen hinsichtlich Cloud Computing Lösungen. Aufbauend auf den Erkenntnissen der Prospect Theory (Neue Erwartungswerttheorie) wird dabei aufgezeigt, dass insbesondere unerfahrene Entscheidungsträger bei der Bewertung einer cloud-basierten Ablösetechnologie stärker von der Bewertung der bestehenden Technologie beeinflusst werden. Durch dieses Status Quo-Denken wird die neue Technologie negativer eingeschätzt, wodurch ihre potenziell vorteilhafte Einführung behindert wird.

Artikel B widmet sich Entscheidungsprozessen im Zusammenhang mit Datenschutzverhalten von Endnutzern und der Auswirkung von „Psychological Ownership“ (Psychologisches Eigentum) auf die Schutzmotivation. In einer Fragebogenstudie und aufbauend auf der Schutzmotivationstheorie wird der Einfluss von Psychological Ownership auf das Entscheidungsverhalten

von Personen sowohl im privaten als auch im beruflichen Kontext analysiert. Dabei wird aufgezeigt, dass psychologisches Eigentumsgefühl stärkere Auswirkungen auf die Schutzmotivation der Teilnehmer in einem privaten Kontext hat, während im beruflichen Kontext insbesondere Eigenverantwortung hinsichtlich der gewählten Schutzmaßnahmen aufgegeben wird.

In Artikel C werden zuvor demonstrierte, kognitive und verhaltensbezogene Aspekte bei Entscheidungsprozessen in einen holistischen konzeptionellen Rahmen verordnet. Basierend auf einer umfassenden Literaturanalyse sowie einer Interviewstudie, wird aufgezeigt, dass Entscheidungen hinsichtlich der IT-Sicherheit in Unternehmen von organisatorischen, ökonomischen, umgebungsbedingten sowie kognitiven und verhaltensbezogenen Aspekten geprägt werden. Dabei wird deutlich, dass der Großteil der bestehenden IT-Sicherheitsforschung trotzdem insbesondere ökonomische Aspekte analysiert. Studien, die IT-Sicherheitsentscheidungen aus einer Verhaltens-, Umwelt-, oder Organisationsperspektive beleuchten, sind deutlich seltener – obwohl die Analyse der Experteninterviews den Einfluss exakt dieser Aspekte hervorhebt.

In Artikel D wird ebenfalls aufgezeigt, dass Entscheidungsträger in Unternehmen von einer Vielzahl von Aspekten bei Investitionsentscheidungen in die IT-Sicherheit beeinflusst werden. In diesem Artikel sowie in Artikel E liegt der Fokus auf Entscheidungsträgern aus kleinen und mittelgroßen Unternehmen, sogenannten KMU. Die Auswertung einer tiefgreifenden Literaturrecherche von existierender Forschung im Bereich organisatorischer IT-Sicherheit zeigt allerdings, dass organisatorische IT-Sicherheit in KMU nur selten systematisch analysiert wurde. Die Auswertung der im Rahmen der Studien in Artikel D und Artikel E durchgeführten Experteninterviews zeigen allerdings auf, dass sich Ergebnisse existierender Forschung aufgrund der Besonderheit des KMU-Kontexts nur bedingt übertragen lassen. Die besonderen KMU-spezifischen Merkmale in Bezug auf IT-Sicherheit werden deswegen untersucht und können validiert werden. Dadurch wird aufgezeigt, dass Investitionsentscheidungen im Hinblick auf organisatorische IT-Sicherheit stark von KMU-spezifischen Merkmalen, wie mangelnder IT-Budgetplanung, undokumentierter Prozesse oder Doppelrollen aufgrund von Ressourcenmangel, beeinflusst werden.

Diese Dissertation liefert folglich wertvolle Erkenntnisse für Praxis und Forschung zu typischen und häufigen Entscheidungsprozessen im Rahmen der Digitalen Transformation. Hervorzuheben sind insbesondere der Einfluss von Wahrnehmungsverzerrungen und nicht reinrationalen Faktoren bei der Entscheidungsfindung hinsichtlich neuer Technologien oder Maßnahmen zur Sicherstellung deren Sicherheit sowie die Auswirkungen von KMU-spezifischen Maßnahmen, die es im Rahmen zukünftiger Forschung zu beachten gilt.

Acknowledgements

This thesis evolved during my work as a research and teaching assistant at the Chair of Information Systems | Software & Digital Business at Technische Universität Darmstadt, Germany. Completing this dissertation would not have been feasible without the moral and active support of many dear colleagues, friends, family, and my supervisor. To express my sincerest gratitude, I dedicate the following acknowledgements to these wonderful individuals.

First and foremost, I am deeply grateful to my supervisor, Prof. Dr. Peter Buxmann, who took a chance on someone with a limited background in information systems and supported me throughout the completion of this thesis and beyond. In addition to his direct guidance and encouragement, I would also like to express my gratitude for his innate sense of building an exceptionally great team of individuals who complement and endorse each other. Even though all of my colleagues deserve to be recognized individually, I would like to highlight my co-authors Dr. André Loske, Dr. Rabea Sonnenschein, Dr. Jin Gerlach, Christian Olt, Luisa Pumplun, Christoph Tauchert, and Jennifer Bornholt. I am deeply grateful for their support, valuable feedback, and our trusting and fruitful collaboration. My initiation into research was superbly guided by André and Rabea with whom I enjoyed great teamwork and conversations. Additionally, I feel highly indebted to Jin, who continuously represented the highest standard of research ethos for me and was an invaluable mentor and an excellent team player throughout our collaborative projects and as a postdoctoral researcher with the faculty. Likewise, I want to express my sincere gratitude to Christian for always ensuring outstanding and trusting cooperation and exceptional project management skills. In the same way, I would like to thank Luisa, Chu, and Jennifer for their fantastic feedback and their immense engagement during our joint research projects. I am also very grateful to Prof. Dr. Alexander Benlian, who accepted the co-supervision of my thesis and provided excellent constructive feedback during doctoral colloquia.

Additionally, each and every member of our research group deserves to be mentioned by name and I would like to thank them for years of interesting, thought-provoking, and empowering

discussions and the valuable feedback they provided on my research: Adrian, Alexander, Amina, André, Christian, Christoph, Esther, Felix, Hendrik Jennifer, Jin, Katrin, Luisa, Melanie, Neda, Nicole, Nihal, Nora, Olga, Ruth, Thomas, Timo K., Timo S., Torben, Ute, and Verena.

Last, but certainly not least, I would like to thank my dearly beloved family and my partner. Their incessant support, approval, and sympathy provided me with the mental stamina and tenacity during demanding times. I cannot thank them enough: my nephew Maxim for making me appreciate the little things in life, my sister Maria for her unquestionable support and constant encouragement, my father Michael for believing that success is just the default setting, my mother Katharina for being the best role model a daughter could wish for, and Romain for his infinite patience and capacity to reassure and comfort me.

Every single individual mentioned above gave me the strength to persist through challenging times and contributed greatly to the completion of this dissertation.

"Soyons reconnaissants aux personnes qui nous donnent du bonheur; elles sont les charmants jardiniers par qui nos âmes sont fleuries."

Marcel Proust (Les Plaisirs et Les Jours, p.35)

Content Overview

Table of Contents

List of Figures

List of Tables

List of Abbreviations

AI	Artificial Intelligence
AIS	Association on Information Systems
AISEL	Association on Information Systems Electronic Library
AVE	Average Variance Extracted
AMCIS	Americas Conference on Information Systems
BMBF	Bundesministerium für Bildung und Forschung
BS	British Standard
CBA	Cost-Benefit Analysis
CEO	Chief Executive Officer
CIA	Confidentiality – Integrity - Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CR	Composite Reliability
CRM	Customer Relationship Management
ECIS	European Conference on Information Systems
EJIS	European Journal of Information Systems
ERP	Enterprise Resource Planning
GDPR	General Data Protection Regulation
H	Hypothesis
HICSS	Hawaii International Conference on System Sciences
IaaS	Infrastructure as a Service
ICIS	International Conference on Information Systems
IDC	International Data Corporation
IEC	International Electrotechnical Commission
IS	Information System(s)
ISIC	International Standard Industrial Classification
ISJ	Information Systems Journal
ISO	International Organization for Standardization
ISR	Information Systems Research
IT	Information Technology
JAIS	Journal of the Association for Information Systems
JIT	Journal of Information Technology

JMIS	Journal of Management Information Systems
JSIS	Journal of Strategic Information Systems
MD	Managing Director
MGA	Multi-Group Analysis
MIS	Management of Information Systems
MISQ	Management of Information Systems (MIS) Quarterly
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
PaaS	Platform as a Service
PACIS	Pacific Asia Conference on Information Systems
PBC	Perceived Behavioral Control
PLS	Partial Least Square
PM	Project Management
PMT	Protection Motivation Theory
PO	Psychological Ownership
PF	Provider Firm
RoI	Return on Investment
RQ	Research Question
SaaS	Software as a Service
SD	Science Direct
SMB	Small and Medium Business
SME	Small and Medium-sized Enterprises
SNS	Social Network Services
SIGSVC	Special Interest Group on Services in the AIS
TAM	Technology Acceptance Model
UF	User Firm
UPF	User and Provider Firm
USD	US Dollar
USITC	United States International Trade Commission
UTAUT	Unified Theory of Acceptance and Use of Technology
TRA	Theory of Reasoned Action
TBP	Theory of Planned Behavior
VHB	Verband der Hochschullehrer für Betriebswirtschaft e.V.
VIF	Variance Inflation Factor
WI	Wirtschaftsinformatik
WTO	World Trade Organization
WoS	Web of Science

1 Introduction

"[…] if a company doesn't invest and it keeps saying 'no' it will begin to lose capability and run behind—suddenly it isn't able to compete. The interesting problem today is, we do a whole lot less bricks-and-mortar-type projects and a whole lot more IT projects, as we've moved from one environment to another."

Warren McFarlan, 2016, Albert H. Gordon Professor of Business Administration, Emeritus, Harvard Business School (in Milovich, 2019)

1.1 Motivation

Today, information technology (IT) is not only seen as a support function to reach strategic business goals but is rather regarded as an enabler that permeates the entire value chain of organizations (Hess et al., 2016). Whereas technology was primarily internally integrated and exploited locally in the last century, it is now redesigning business processes, value chains, and networks, or even redefining the scope of businesses through new business models (Veit et al., 2014; Venkatraman, 1994). In this constant state of flux, managers and executives need to continuously change to compete, adopt new requirements to adapt to them, and invest to improve existing operational processes. They are constantly faced with a multitude of potentially business-critical decisions. Management principles and managerial decisions, in particular, are thus at the very core of the so-called digital transformation. Cognitive psychologist and Nobel Prize laureate Herbert Simon even states, "I shall find it convenient to take mild liberties with the English language by using 'decision-making' as though it were synonymous with 'managing'" (Simon, 1960). The decision-making process, as outlined by Herbert Simon (1960), comprises three phases: (1) intelligence activity, (2) design activity, and (3) choice activity. These activities can also be embedded easily in more extensive models, such as Huber's problem-solving model, which supplements Simon's process by adding the phases (4) implementation and (5) monitoring, as depicted in Figure 1 below.

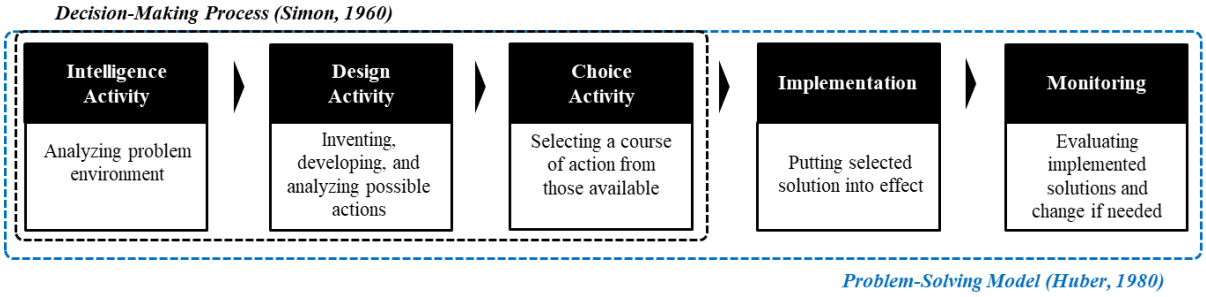

Figure 1. Phases in the Managerial Decision-Making Process (based on Simon (1960) and Huber (1980))

Since decisions are at the core of all managerial activities and play a decisive role in ongoing digital transformation processes, improving the understanding of organizational decisions in an information systems context is crucial for information systems (IS) research.

The realm of IS research—as stated by Hevner and colleagues (2004, p. 77)—is at the confluence of people, organizations, and technology. Since it covers such a wide array of topics, the IS discipline has often been regarded as an applied discipline drawing upon more mature reference disciplines, such as computer or management science, economics, or behavioral decision theory (e.g., Bakos & Kemerer, 1992; Keen, 1980). Consequently, the analysis of decision-making processes in IS research has often drawn on existing research and has inherited one of its most accentuated dividing lines, which distinguishes between "behavioral IS" and "economics of IS" (Goes, 2013).

Even though decisions and their consequences are at the core of these reference disciplines, economics—defined by Simon (1959) as "the science that describes and predicts the behavior of several kinds of economic man" (p.253)—and behavioral science, which encompasses (cognitive) psychology and decision science, have largely evolved disparately. According to Simon (1959), economists until the 1960s predominantly focused on normative macroeconomics, in other words, analyzing industries and the entire economy to guide public policy decisions. Normative research, in contrast to descriptive research, assesses reality and actions relative to the standard or an ideal. The "economic man" is assumed to be a rational, completely informed actor following the tenets of rational choice theory. Therefore, economists were interested in how individuals or organizations *should* or *ought* to behave and decide. The informed decision-maker is aware of all possible alternatives and knows their consequences and can, therefore, attach numerical values or weights to each alternative when faced with a decision. Ultimately, the alternative with the highest expected value or utility will be selected. However, Simon (1979) and other behavioral scientists such as Huber (1981), Das and Teng (1999), Klein

(2017), or Chase and colleagues (1998) have continuously argued for theories of decision-making accounting for incompleteness of information, uncertainty and risk, or constraints of human rational behavior.

Experimental methods modeling decision-making under risk have demonstrated that actual human behavior and decisions violate the axioms of the economic concept of utility, leading to the development of prospect theory (Kahneman & Tversky, 1979) and the emergence of behavioral economics. As such, the descriptive approach when analyzing and explaining behavior and decision-making processes, which accounts for the perceptual and cognitive processes of the "economic man" or decision-maker and the incompleteness of information and constraints, has received increased research interest in various disciplines. Decisions and decision-makers do not exist in a "vacuum" but are highly affected by contextual factors. Since context in the IS environment is rapidly changing and, consequently, more complex than previously analyzed environments, IS research can benefit from analyzing decisions with a descriptive approach informed by findings from behavioral science.

1.2 Research Questions and Objectives

Decision-making processes are at the heart of each research study included in this dissertation. All studies were published in proceedings of various well-known and distinguished international conferences or in an IS journal. As such, they all cater to the scientific community as well as to practitioners and private individuals, since the addressed research questions entail ramifications for society, academia, and business. Both the discussion of the respective limitations as well as potential future research avenues are designed to help advance further studies regarding decision-making in the age of digital transformation. Subsequently, all research questions and associated objectives are presented briefly. Further detailed presentations of questions and objectives as well as how these are situated within the broader IS research landscape can be extracted from Chapters 4–8.

As pointed out in the motivation, organizational decision-makers do not adhere to the tenets postulated by rational choice theory but experience limitations of rationality, especially in uncertain or highly complex situations. A common decision-making approach in such a situation is the application of heuristic problem-solving technique or so-called cognitive shortcuts (Simon, 1997; Tversky & Kahneman, 1975). Various studies in economics or, more specifically, in IS, have demonstrated that individuals are affected by biases when assessing risk (e.g., Fleischmann et al., 2014; Samuelson & Zeckhauser, 1988; Tversky & Kahneman, 1975). When

assessing the perceived risk of cloud computing, Loske and colleagues (2014), for example, could demonstrate the influence of unrealistic optimism and stark differences between users and providers. The influence of such biases was also uncovered in the broader areas of IT security risk management (e.g., Rhee et al., 2012; Tsohou et al., 2015). The majority of studies analyze biases in comparison to other individuals or organizations, while prospect theory postulates that, when faced with uncertainty, individuals generally draw on reference points. An organizational decision-maker will thus not (solely) compare a new solution—in this case, represented by a software as a service (SaaS) solution—to other companies but also to the technology in place, in other words, the status quo or incumbent technology. Consequently, previous experience with the potential new technology could serve as a reference point for assessing the risks and benefits of such a replacement or adoption decision. The use of such a reference point is referred to as status quo thinking, leading to status quo bias (e.g., Kahneman et al., 1991; Samuelson & Zeckhauser, 1988; Schweitzer, 1995). The first research question in Chapter 4, therefore, investigates if and how status quo bias can be observed in technology adoption decisions:

> ***RQ 1****: How does status quo thinking influence managers' decisions in adopting new IT systems?*

When assessing cloud computing solutions, one of the perceived risks that tends to be most frequently mentioned, and that weighs quite heavily in decision-making, is the security risk. To better understand the perception and role of security risks in decision-making, the following studies in Chapters 5–8 focus on behavioral, economic, organizational, and environmental aspects in decision-making processes regarding IT security or data protection as part of the "intelligence activity" phase outlined above and illustrated in Figure 2 below.

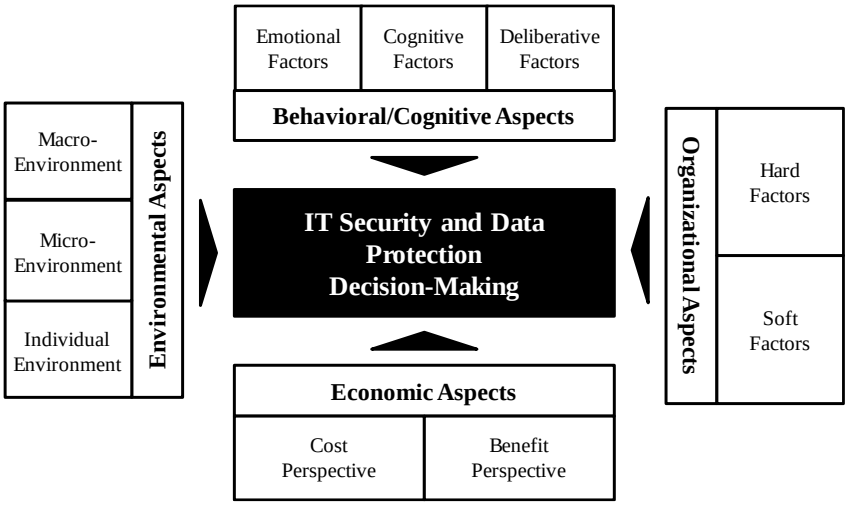

Figure 2. General Framework of Aspects in Decision-Making Processes

Whereas economic aspects of decision-making have been rather prominent in the analysis of decision-making in general and in decisions regarding IT security in particular (e.g., Cavusoglu et al., 2004; Khansa & Liginlal, 2009), other aspects have attracted less scrutiny (e.g., Crossler et al., 2013) or are solely analyzed in either a work environment or in the context of private use (e.g., Lebek et al., 2014; Mayer et al., 2017; Mou et al., 2017).

Context is king, however, as explicated in detail by Davison and Martinsons (2016), who argue that the scope of validity for research findings and implications depends heavily on the context of the respective empirical research. In this regard, conclusions derived in studies analyzing individual IT security behavior in a private-use context cannot necessarily be confirmed in a work-environment context. Following the call of Crossler and colleagues (2013), the study in Chapter 5 sets out to analyze how behavioral aspects such as the feeling of psychologically owning data might affect the decision to protect data in both contexts. Psychological ownership has been analyzed in various contexts, including its impact on protection motivation among employees (Menard et al., 2018), but was never contrasted and compared with the impact on the same behavior in a private-use context. The second research question in Chapter 5, therefore, investigates if and how psychological ownership impacts data protection decisions in two different situational contexts:

> ***RQ 2**: How does psychological ownership affect the decision to protect data, and does the influence of psychological ownership differ according to situational differences in contexts?*

As mentioned above and pointed out by IS researchers such as Paulo Goes, Management Information Systems Quarterly editor-in-chief emeritus (2013), or Crossler and colleagues (2013), findings from behavioral economics and decision sciences have not been adopted sufficiently in IS research.

Especially in organizational IT security research, decision-making is still often approximated with normative statistical decision theories despite the frequently stated and proven importance of contextual factors (e.g., Angst et al., 2017; Cavusoglu et al., 2015; Dhillon & Backhouse, 2001; Straub & Welke, 1998). Therefore, it is necessary to consider contextual factors in security and privacy studies, given the highly complex nature of current IS environments. Drawing on previous research by Dor and Elovici (2016), these factors can be grouped into behavioral/cognitive, organizational, environmental, and economic aspects as demonstrated in Figure 2. Organizational IT security decisions consist of multiple steps or phases that follow the managerial decision-making process as outlined in Figure 1. These steps have been successfully applied to the IT security context by Straub and Welke's (1998) security risk planning model

as well as through the model for managerial perceptions of security risk by Goodhue and Straub (1991). By combining and integrating these theoretical decision frameworks, the third research question in Chapter 6 sets out to analyze which contextual aspects are most prevalent during which specific decision phase and additionally scrutinizes how much they have been considered by extant research:

> ***RQ 3**: Which contextual aspects affect decision-makers during the decision-making process regarding organizational IT security, and to what extent has previous research considered these contextual aspects?*

The analysis of extant research in Chapter 6 also unveils another area of scarce research: IT security research focusing on small and medium-sized enterprises, which represent the vast majority of enterprises globally (e.g., Angst et al., 2017), even though IT security investments in SMEs are still lagging behind larger organizations and ultimately result in ever more damaging security incidents. Despite being denounced as the "weakest link in the security chain" or the gateway for wrongdoers, IS research has largely overlooked these enterprises or disregarded specific constraints that would impact the generalizability of extant research implications (Davison & Martinsons, 2016). Previous IS studies focusing on the adoption of information technologies of SMEs have demonstrated that SMEs face several specific constraints and share characteristics that affect their decision-making processes (e.g., Eikebrokk & Olsen, 2007; MacGregor, 2003; Thong, 1999; Thong & Yap, 1995). Due to the scarcity of IT security research placing SMEs at the center of attention, the influence of such characteristics and constraints on decisions regarding IT security (investment) remains unclear. The fourth research question, therefore, postulates:

> ***RQ 4**: Which SME constraints influence organizational IT security, and how do these identified SME constraints manifest themselves and influence IT security (investment) decisions?*

The so-called security divide between large enterprises and SMEs is also the subject of the last paper in Chapter 8 concluding this dissertation. Increasing damage from cyber security breaches affecting SMEs (Zurich, 2017) and the results of the study in Chapter 7 also imply that existing findings of IT security studies may not paint the full picture by disregarding SME-specific characteristics and constrains. As demonstrated by the literature review in the abovementioned study, only a single IS security study in the Association for Information Systems Senior Scholars' basket of eight, which comprises the most prestigious IS research outlets, places the spot-

light on SMEs (Lee & Larsen, 2009). Extending the literature review by including articles published in additional esteemed IS journals, the fifth research question aims to identify how well previous research has accounted for SME-specific influencing factors:

> ***RQ 5*** *How do internal SME-specific firm characteristics or external pressures and barriers affect their IT security investments, and to what extent has previous IS security research considered the influence of these SME constraints?*

The following section provides an overview of the featured research articles and where they were published, along with a more thorough description of the overall structure of this dissertation.

1.3 Structure of the Thesis

This thesis includes five papers, all of which address decision-making in the context of several processes and initiatives that organizations face during their digital transformation journeys. They are listed and summarized below.

Papers focusing on cloud computing or SaaS adoption decisions:

- **Paper A:** Heidt, Margareta; Sonnenschein, Rabea; Loske, André (2017): **Never Change a Running System? How Status Quo Thinking Can Inhibit Software as a Service Adoption in Organizations**. In: Proceedings of the 25th European Conference on Information Systems (ECIS), Guimarães, Portugal. VHB ranking: **B**. **SIGSVC (Special Interest Group on Services in the AIS) Best Paper of the Year Award.**

Papers focusing on data protection and IT security investment decisions:

- **Paper B:** Heidt, Margareta; Olt, Christian M.; Buxmann, Peter (2019): **To (Psychologically) Own Data is to Protect Data: How Psychological Ownership Determines Protective Behavior in a Work and Private Context.** In: Internationale Tagung der Wirtschaftsinformatik (WI), Siegen, Germany. VHB ranking: **C.**
- **Paper C:** Heidt, Margareta; Gerlach, Jin; Buxmann, Peter (2019): **A Holistic View on Organizational IT Security: The Influence of Contextual Aspects During IT Security Decisions.** In: Hawaii International Conference on System Sciences (HICSS), Wailea, USA. VHB ranking: **C**.
- **Paper D:** Heidt, Margareta; Gerlach, Jin (2018): **The Influence of SME Constraints in an Organizational IT Security Context.** In: Proceedings of the 39th International Conference on Information Systems (ICIS), San Francisco, USA. VHB ranking: **A**.

- **Paper E:** Heidt, Margareta; Gerlach, Jin P.; Buxmann, Peter (2019): **Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments.** In: Information Systems Frontiers, 21, pp. 1285–1305. VHB ranking: **B.**

The remainder of this section provides an overview of each paper's content and emphasizes how they relate to this dissertation's research goals.

Paper A analyzes decision-making processes of managers when faced with the adoption of a new technology, in other words, software as a service (SaaS). This paper places an emphasis on status quo thinking of managers, drawing on prospect theory and previous research regarding heuristics and biases (Kahneman & Tversky, 1979). In particular, the developed research model aims to explain and test the influence of the respective incumbent technology, likely an on-premise solution, on the evaluation of benefits and risks associated with SaaS. This derived model is then empirically tested based on a data set of 123 managers gathered via an online survey. The results indicate that the attitude toward SaaS, or a new technology in general, largely depends on the perceived benefits and risks attributed to the current, incumbent system and the potential first experience with the new technology. The latter is assessed via the existing degree of SaaS adoption in the respective organization. The less experience managers could gather with SaaS, the more heavily their assessment is impacted by their evaluation of the existing technology. Lacking exposure to the new technology increases the impact of status quo thinking, as these managers tend to overvalue risks associated with the new technology and, therefore, favor the retention of the incumbent technology. Prospect theory explains this overestimation as loss aversion, which ultimately inhibits the potentially beneficial adoption of a new technology.

Paper B addresses the question of how the sole feeling of ownership toward an intangible target such as data can lead to heightened levels of the individual's perceived responsibility. Drawing on organizational research, this paper investigates whether and to what extent this feeling of ownership differs between personal files and data accessed in the work context. Against the backdrop of ever-rising rates of data generation and associated security risks, data protection continues to attract both organizational and individual interest. In addition to technical measures, typical data protection measures such as password authentication revolve around end-users, who are often described as the weakest link in the information security chain. Drawing on organizational research—which argues that the sole feeling of ownership toward an intangible target, such as data, can lead to heightened levels of the individual's responsibility—

this paper investigates whether and to what extent this ownership feeling differs between personal files and data accessed in the work context. Drawing on data derived through a two-phase questionnaire among a representative group of 209 employees, psychological ownership exerts stronger effects on protection motivation among participants in a private context. The results also indicate that responsibility for data protection is partly relinquished in the work context, which represents a key aspect of developing feelings of psychological ownership.

Paper C integrates previously discussed behavioral aspects into a proposed decision-making framework focusing on IT security (investment) decisions. Based on findings from organizational and behavioral science and 25 expert interviews, this framework depicts the influence of contextual aspects such as organizational, environmental, economic, cognitive, and behavioral aspects of decision-makers. Building on Straub and Welke's (1998) security risk planning model and the previously postulated conceptual framework, a critical literature review of organizational IT security literature reveals, however, that decisions are predominantly approximated by models drawing on normative statistical decision theories. The paper thus highlights the scarcity of studies analyzing IT security decision-making from a behavioral, environmental, and organizational perspective and argues for the importance and future consideration of contextual aspects regarding IT security decisions.

In *Paper D*, the effect of contextual aspects on organizational IT security investment is further investigated. Moving away from the security risk planning model (Straub & Welke, 1998), this paper focuses on SME-specific characteristics and finds that organizational IT security research has largely neglected SMEs or superimposed certain theoretical assumptions that are not necessarily applicable in an SME context. Based on a literature review and a resulting conceptualization of general SME characteristics, several constraints are validated and contextualized regarding their influence on IT security investment decisions through 25 expert interviews. The findings strongly suggest that several widely held assumptions in extant IT security literature should be modified if researchers claim generalizability of their results in an SME context. Exemplary assumptions include the existence of formalized, documented processes or IT budget planning, which are often nonexistent or underdeveloped in SMEs. Additionally, this study offers 14 propositions regarding the particular effects of identified constraints on IT security investment decisions in SMEs for future IT security research.

Paper E represents an extension of Paper D with a more granular analysis of the previously identified constraints. This paper additionally includes a structured literature review that

demonstrates that organizational IT security research in an SME context has been largely neglected. The findings imply that several widely held assumptions in extant IT security literature should be modified if researchers claim generalizability of their results in an SME context. Exemplary assumptions include the presence of a skilled workforce, documented processes, or IT budget planning, which are often un(der)developed in SMEs. Additionally, the study offers context-specific insights regarding particular effects of identified constraints on IT security investments for all involved stakeholders (researchers, SMEs, large enterprises, and governments).

2 Theoretical Background

This section provides an overview of the theoretical fundamentals in addition to the theoretical background section of each subsequently featured paper. While the first part introduces the term "digital transformation," the second part refers to cloud computing, and the last section provides a brief overview of information security aspects in IS research.

2.1 Digital Transformation

Ever since its inauguration in 1977, the first dedicated journal for IS, the *Management of Information Systems Quarterly* (MISQ), states its mission as follows: "Enhancement and communication of knowledge concerning the development of IT-based services, the management of IT resources, and the use, impact, and economics of IT with managerial, organizational, and societal implications" (MIS Quarterly, 2019).

In one of the two interviews that are included in the first MISQ issue, the president and director of the North Carolina National Bank Corporation (today, Bank of America), William Dougherty, predicted eerily detailed changes that he expected to see regarding how information will be provided to business executives: "I think it will be changing more in the amount of material coming in. The reams of paper will be disappearing […]. I think the other area is more online information at our fingertips. This relates to automation where we can interface with the computer and get information more quickly" (Halbrecht, 1977).

Long before the term was actually coined, Dougherty describes the tenets of digitization, in other words, "the process of changing from analog to digital form" (Gartner, 2019), where information saved on paper will increasingly disappear in favor of digitized copies. Furthermore, Dougherty also predicts the notion of ubiquitous computing and its influence on the way we work—in other words, how information or technology transforms the way individuals and organizations operate.

The latter description is a common aspect of the term "digital transformation." In an extensive literature research, Morakanyane and colleagues (2017) define the term as "an evolutionary process that leverages digital capabilities and technologies to enable business models, operational processes, and customer experiences to create value" (p.437). As such, enabling digital transformation has been an integral objective for top executives globally (Hess et al., 2016). To reap the benefits of successful digital transformation initiatives, organizations must establish adequate management practices and define an overarching strategy that ties in with operational

and functional strategies. Consequently, executives and decision-makers need to identify how to balance (1) the use of technologies, (2) the changes in value creation, (3) structural changes, and all related (4) financial aspects. In this regard, a decision to introduce a certain technology is not simply determined by the expected investment costs and return on investment (RoI), but it also impacts processes and could redefine an organization's product and service portfolio, thus, its overall value proposition. Against this backdrop, executives and researchers have encountered various digital capabilities and technologies, each promising to be "the next big thing." Unsurprisingly, several studies have demonstrated that making technology investment and adoption decisions constitutes a consistent challenge for executives (e.g., Adomavicius et al., 2008; Gomber et al., 2018; Gurbaxani & Whang, 1991). The decision to invest and introduce a new technology is laden with ethical considerations involving security and privacy; legal questions regarding regulations, policies, and the governing law; organizational and personal phenomena regarding the adoption and habituation; and the assessment of threats, vulnerabilities, and procedural integration (Lowry et al., 2017). One compelling example for such a technology that encompasses the aforementioned considerations is cloud computing. Often referred to as one of the key enablers of digital transformation, the mass provision of data storage and processing via cloud computing is discussed in further detail in the following section.

2.2 Cloud Computing

Scholars and practitioners alike have hailed cloud computing as a paradigm shift (e.g., Urquhart, 2008; Yang & Tate, 2012). According to the U.S. National Institute of Standards and Technology (NIST) definition as provided by Mell and Grance in 2011, cloud computing is commonly understood as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011, p. 2). Typically, this definition also states four deployment models (private cloud, public cloud, community cloud, and hybrid cloud), three main service models (infrastructure as a service, platform as a service, and software as a service), and five essential characteristics as depicted in Figure 3 below. Per definition, cloud computing (1) is an *on-demand self-service* where consumers can unilaterally provision computing capabilities as needed, (2) offers *broad network access* through standard mechanisms promoting use by client platforms, (3) allows multiple clients to use the provider's computing resources via *resource pooling* of storage, processing, memory, virtual machines,

and network bandwidth, and (4) features *rapid elasticity* to quickly provision or scale capabilities (Mell & Grance, 2011; Yang & Tate, 2012).

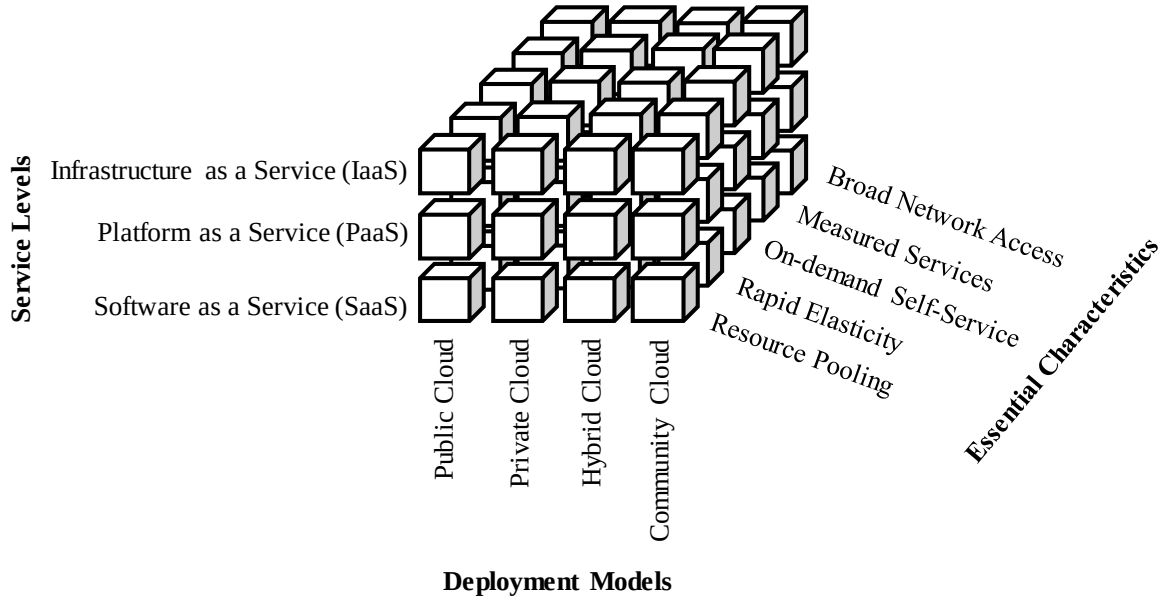

Figure 3. Cloud Computing Anatomy (adapted from Yang and Tate (2012), based on Craig-Wood (2010))

Originally, the term "cloud computing" mainly referred to the public cloud deployment model where a vendor operates the cloud capabilities and makes these available to the general public, in other words, multiple clients via a multi-tenant architecture. Other deployment models are variations sharing a similar technological base but differing in terms of the relationship between provider and clients or consumers. In a private cloud relationship, cloud capabilities are managed and maintained in-house or on the premises and, thus, are exclusively accessible for internal users of a specific customer organization. The community cloud variation sits between the public and private models, as it is a multi-tenant structure for several specific organizations that form a defined community with shared policies and requirements. A combination of either of the previously mentioned deployment models can be described as a hybrid cloud model. Exemplary for hybrid cloud deployment models are organizations that are highly regulated—such as financial institutions or the pharmaceuticals industry—and, as a result, need to exercise strict security requirements for a certain area, department, or specific data sets that can only be stored and processed via a private cloud that is managed in-house. Since public clouds can often be more easily scaled and might offer cost advantages, the aforementioned organizations might store less-sensitive data on a public cloud or access their customer relationship management (CRM) system—an example of an SaaS application—via a public cloud.

The latter example of a CRM system delivered as an SaaS, an off-the-shelf application that can be accessed by (organizational or private) users through the internet, represents one of the three service layers of cloud computing. Organizations usually enter a subscription contract with an SaaS provider to access a service application that continues to be maintained by the provider or must be run on in-house servers. An SaaS application is usually fully managed by the provider or vendor who has full control over servers, storage, networking, operation system, virtualization, middleware, runtime, applications, and data. More control, specifically regarding applications and data, is available to organizational users in the service layer platform as a service (PaaS). A PaaS environment enables users to run, develop, and even distribute their own applications via associated marketplaces offered by PaaS providers. PaaS provision usually includes a complete development environment based on the provider's cloud infrastructure that is still managing runtime and delivering necessary middleware. The latter two are managed only by the user itself in an infrastructure as a service (IaaS) agreement, where the respective IaaS provider offers virtualization, raw processing power, data storage, and networking capabilities.

One key differentiator of cloud computing compared to traditional internal or in-house provisioning of computing resources is the scalability on demand, which is enabled through dynamic pay-per-use pricing models defined in the subscription agreements between providers and users. As such, cloud computing can be understood as IT outsourcing, as it helps users "to satisfy their needs for efficiency, cost reduction, and flexibility" (Leimeister et al., 2010, p. 7). Organizations can minimize their fixed IT costs and can continue to service their own customers efficiently, quickly, and flexibly, since computational resources are readily available and scalable. This ultimately enables organizations to introduce potentially disruptive, innovative services to their customers with a shorter time-to-market and ultimately leads to new business models: Organizations can build on mature toolsets without large upfront investments to meet or exceed customer expectation (Müller et al., 2015). The benefits of cloud computing can be reaped in several levels throughout the business-IT-maturity level (based on Pearlson & Saunders, 2007) as identified by a literature review of Müller and colleagues (2015). The first level refers to increasing business efficiency through cost reduction and business process efficiency, whereas the second level describes how business effectiveness is improved via enhanced intra-enterprise collaboration, business integration, and IT infrastructure, along with a focus on core competencies. The third level summarizes how cloud computing leads to innovation and business transformation via business growth through innovative services and products, agile capabilities, and increased business partner collaboration. The latter is enabled through cloud computing, as it helps increase information sharing and enables knowledge networks across the

value chain by connecting stakeholders through shared systems and greater available (shared) data.

However, these benefits are also associated and can be outweighed by risks and costs inherent in the cloud computing model. Based on a large-scale survey of 349 IT executives at German companies, Benlian and Hess (2011) have demonstrated the influence of perceived risks and opportunities of SaaS adoption on the intention to increase the current level of SaaS adoption. Their model assesses the influence of salient opportunity beliefs around cost advantages, strategic flexibility, a focus on core competencies, access to specialized resources, and quality improvements as well as salient risk beliefs regarding performance, economic risks, strategic risks, and managerial risks. Whereas IT executives are not swayed significantly by managerial risks, economic, performance, and strategic risks did affect their intention. However, security risks—such as data loss, theft, or corruption—were identified as an especially dominant factor in influencing the intention to further adopt SaaS.

The call for increased data protection and security is not exclusive in cloud computing provisioning but has become louder against the backdrop of ever-increasing reliance on computational resources of both organizations and private individuals. Rising numbers of data breach incidents and their associated losses have also heightened the overall security demand. Whereas cloud computing can be regarded as an enabler for digital transformation, information security and data protection have had a more diverse or sometimes more ambiguous role—as inhibitor, constraint, goal, or cornerstone—which is reviewed in the following section.

2.3 Information Security

According to NIST, information security is defined as “the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability” (Paulsen & Byers, 2019). Similarly, the International Standard ISO/IEC 27000 also defines information security as the “preservation of confidentiality, integrity, and availability of information” with other properties being potentially involved, for example, authenticity, accountability, non-repudiation, and reliability (ISO, 2018, p. 4). The so-called CIA triad is a common abbreviation to describe the three tenets of information security, in other words, (C) **confidentiality**, to assure that information is not disclosed to unauthorized individuals or processes; (I) **integrity**, to guard against improper modification or destruction of information; and (A) **availability**, to ensure timely and reliable access to and use of information (Paulsen & Byers, 2019).

Information security has received widespread attention in both IS research and IS practice, especially when studies address a substantial security or privacy problem at the organizational level (Lowry et al., 2017). IS researchers state that security and privacy are even more important today and have received board of directors-level attention due to new developments such as the internet of things (IoT), the increasing adoption of artificial intelligence (AI), and the general increasing dependence of information systems and networks (e.g., Chen et al., 2011; Lowry et al., 2017). Due to the increasing relevance of information and information systems for both individuals and organizations, which provide an ever-growing surface for attack, the sophistication of threats and the associated amplitude, power of impact, and costs are rising continuously (e.g., Barrett, 2019; Salge et al., 2015). Information security and the mitigation and management of IS risk have, however, not only recently become an integral part of the agenda of every chief information officer (CIO) or chief IT security officer (CISO), as demonstrated by various research endeavors (e.g., Schweitzer, 1995; Straub & Welke, 1998; von Solms et al., 1994) and standards or codes of practice such as BS-7799-1 (BS 7799-1:1995, 1995) or ISO/IEC 27001 (2018).

Consequently, information security management has become a cornerstone of organizational risk management along with the guarantee of business continuity and privacy for employees and customers. Whereas security refers to the mechanisms or safeguards established to achieve the confidentiality, integrity, and availability of information and data, privacy is rather seen as a right referring to the appropriate use of personal information as defined by the law, public sensitivity, or respective policies.

Extant research investigating the implementation of information security measures indicates that successful adoption is driven largely by technological, environmental, and organizational factors, but also individual factors. Security breaches and announced IT security investments can, for example, on an environmental level, either lead to absorption of market share and power by unaffected competitive organizations or spur IT security investment among competitors in a contagion effect (Jeong et al., 2019). The role of individuals in information security has received rather widespread attention. On the one hand, employees who often still lack certain skills in risk identification and thus display insecure behavior are placing their organization and associated information and data at risk (e.g., Crossler et al., 2013; Johnston & Warkentin, 2010; Willison & Warkentin, 2013). On the other hand, individuals within organizations are usually also the decision-makers when choosing the implementation of security measures or the adop-

tion of technologies such as cloud computing, which carry innate information security and privacy risks (e.g., Angst et al., 2017; Benlian & Hess, 2011; Lowry et al., 2017). Since many business goals are highly intertwined with organizational information systems, as demonstrated, for example, by the earlier mentioned business-IT-maturity level, every IT investment or outsourcing decision does carry issues and questions around security and privacy, as pointed out by the initially cited IS professor Warren McFarlan (Milovich, 2019).

Despite the high relevance for IS research and IS practice, information security research represents a rather intrusive area of organizational issue as pointed out by Kotulic and Clark (2004), who argue that mass mailings of survey instruments (questionnaires) should be reconsidered an appropriate data-collection method in favor of qualitative research methods such as interviews and case studies. The following chapter thus aims to provide a general overview of relevant research methods and their underlying assumptions as well as how and why the studies of this dissertation follow varying approaches to answer the research questions outlined in Chapter 1.2.

3 Research Assumptions and Methodology

In broad terms, research can be defined as the design process undertaken in a systematic way to identify factors that ultimately increase knowledge (Saunders et al., 2015, p. 5). A systematic way requires a thorough explanation of the chosen approach, the methods, and the strategy applied to collect and make sense of the research data—in other words, a description of the research methodology and the underlying fundamental questions that have led to the chosen research methodology. This overview discusses the approach of each research study included in this dissertation and the scientific toolset, in other words, the concrete methods chosen to answer the research question at hand and, therefore, to ultimately reach the respective research goal.

Research does not exist in a vacuum, consequently, every research endeavor is based on certain assumptions regarding the nature of (1) reality and (2) knowledge, accompanied by (3) the role of ethics and values during the process (Saunders et al., 2015, pp. 124). In the philosophy of science, these assumptions are referred to as the study of being, "**ontology**"; the study of knowledge, "**epistemology**"; and the study of methods themselves, "**methodology**"; and all of these are guided by the values held by the researcher, "**axiology.**" Figure 4 depicts the dependency of these studies: Methodology and the actual chosen methods are defined by the fundamental worldview of the researcher and are thus dependent on the underlying epistemology, which, in turn, is based on a compatible ontology and axiology. From a philosophical point of view, ontology can be understood as an attempt to recognize, name, and order the world of things comprehensively (Busse et al., 2014). Epistemology and axiology are less abstract, since they directly define the relationship between the researcher and the research endeavor, in other words, how knowledge can be generated regarding the research matter and whether the matter is worth investigating.

The most common distinction of possible worldviews in information systems is one between **positivism** and **interpretivism/constructivism** (e.g., Hovorka & Lee, 2010; Weber, 2004). Positivists believe, according to their ontological assumption, that reality is driven by immutable natural laws and that it exists irrespective of our awareness or consciousness, in other words, the individual who observes it (Guba & Lincoln, 1994). According to their epistemological assumption, knowledge must exist beyond the human mind, and the research matter exists independently of the research and can be studied objectively. Therefore, research findings can be classified as either true or false. Interpretivists assume, ontologically, the inseparability of the

observer and the reality; as a result, knowledge creation is always part of the stream of consciousness and life experience that serve as the underlying base of interpreting the research matter (e.g., Klein & Myers, 1999; Weber, 2004). Research findings are uncovered and the researcher is interactively linked with the research matter. Further underlying worldviews in IS and business research are referred to as **post-positivism** and **critical theory** (e.g., Guba & Lincoln, 1994; Myers, 1997; Orlikowski & Baroudi, 1991). **Post-positivism** represents a progression of positivism where reality can only be apprehended imperfectly by the observer. As a result, research findings can never be completely true or false but are rather approximated and are probably true and false. **Critical research,** on the other hand, assumes "that social reality is historically constituted and that it is produced and reproduced by people" (Myers, 1997, p. 5) and that knowledge is thus grounded in social and historical practices (Orlikowski & Baroudi, 1991). A research matter can only be understood when its historical and current development is analyzed (Chua 1986). Depending on the ontological and epistemological assumptions, a researcher would also decide whether the matter is worth investigating and whether the research matter can be approached unbiased or biased, demonstrating the researcher's axiological assumption.

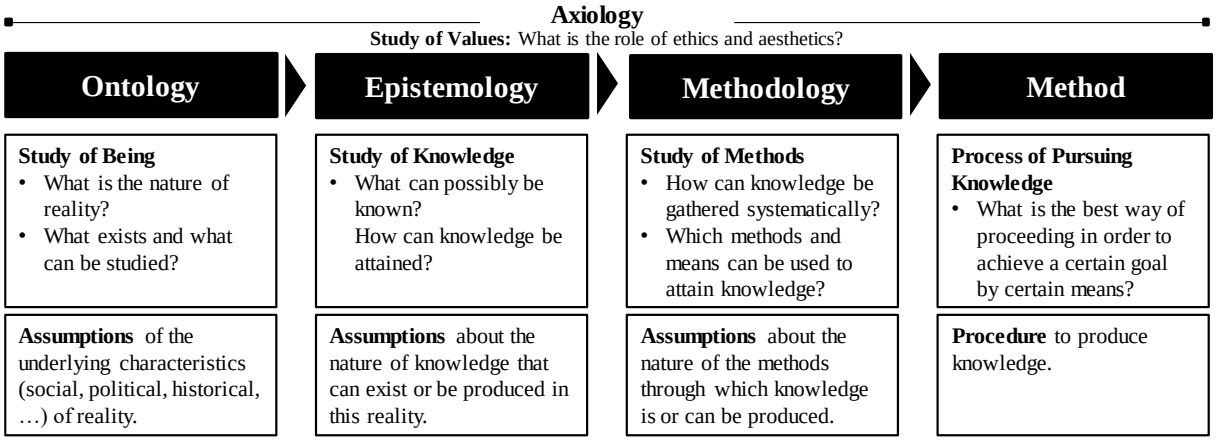

Figure 4. Philosophy of Science and Research Assumptions

Other possible worldview distinctions commonly encountered in business and management or information systems disciplines are **objectivism** and **subjectivism,** or **regulation perspective** and **radical change** (Saunders et al., 2007). These distinctions or underlying **philosophies** are considered as the first "peel" of the so-called research design "onion" based on research by Saunders and colleagues (2007). The research studies of this dissertation can be categorized according to the underlying philosophy, approach, strategy, choice, time horizons, techniques, and procedures as outlined in the research onion (see Figure 5).

The “onion peels” are necessary steps in all research endeavors that inform why a certain data collection or analysis method was chosen to answer the respective research question.

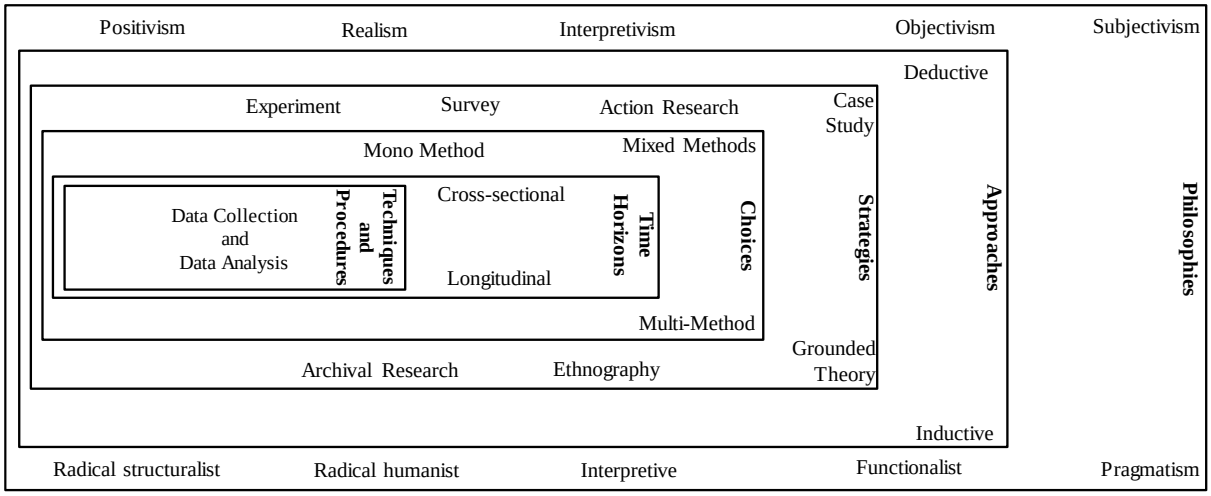

Figure 5. Research Onion (based on Saunders et al. 2007)

The first peel of the research onion refers to the researcher’s **philosophies,** or worldview and assumptions, as described above. The second peel considers the researcher’s overall **approach** to the reasoning: (1) Deductive reasoning attempts to derive a conclusion from a given set of premises or existing literature and theory in a top-down approach, whereas (2) Inductive reasoning embraces a bottom-up approach where the researcher uses observations to detect patterns, which then inform the conclusion or theoretical framework. A third, less common, approach is (3) abductive reasoning, which is triggered through an anomaly or inconsistency of what is known: Whereas deduction aims to verify or falsify theory, induction serves to build theory, abduction is a process, and conclusions derived are not final but may lead to new conclusions or modifications of existing theory (e.g., Saunders et al., 2007; Van de Ven, 2007).

Subsequently, the chosen approach informs the **research strategy** and, thus, the **methodological choice** between a quantitative, qualitative, or mixed method form of research. Quantitative methods are commonly associated with a positivistic stance and deductive approach, since data collected is used to test theory or hypotheses *a priori*. In a mono-method quantitative study, data would be collected to examine and test the expected relationship between variables numerically, in other words, by employing statistical or graphical analyses (Saunders et al., 2007). A multi-method quantitative study would draw on more than one data set, collection technique, and analytical procedure. Typical strategies employed are experiments, surveys, or formal and numerical methods such as econometrics and mathematical modeling. If a quantitative and a

qualitative method are employed, the research draws on mixed methods (sometimes also referred to as triangulation, see Myers (1997)), which—similar to multi-method studies—provide a more holistic approach to data collection and analysis based on richer underlying data. In contrast to quantitative studies, qualitative methods draw on textual data and are often associated with interpretive worldviews and an inductive approach, since they enable the researcher to understand the research matter embedded in a particular context. Common strategies are case study research, action research, ethnography, and grounded theory (Myers, 1997).

Time horizon refers to the time frame the collected data covers: If the data collected for depicting the research matter or measuring a phenomenon was taken at a specific point in time as a snapshot, the time horizon is referred to as cross-sectional. If, on the other hand, data was collected via several snapshots or observations in the form of ongoing diary entries, the time horizon is referred to as longitudinal. The first is often associated with one-time surveys or case studies, whereas the latter is prominent in archival research, ethnographic studies, or repeated surveys or case studies spanning several points in time.

Data collection and analysis are dependent on the previous peels of the research onion: Embracing a post-positivism, researchers would approximate their deduced conclusion with the results of statistical analyses drawing on survey data collected via a questionnaire. This core of the research onion depicts the exact procedure for how knowledge was pursued to ensure rigor and should demonstrate several quality criteria such as reliability and validity, dependability, credibility, and transferability (e.g., Kaplan & Maxwell, 2005; Saunders et al., 2007).

The studies included in this dissertation vary in their philosophical assumptions and the resulting approach and strategy as depicted in the following Table 1. The distinction of the worldviews or underlying philosophical assumptions are, however, not as clear-cut as presented below. When positioned on a continuum, the respective study would rather be located most closely to the mentioned philosophy but may be influenced by other philosophies, bearing in mind that “no construction is or can be incontrovertibly right; advocates of any particular construction must rely on *persuasiveness* and *utility* rather than *proof* in arguing their position” (Guba & Lincoln, 1994, p. 108).

	Paper A	Paper B	Paper C	Paper D	Paper E
Underlying Philosophy	Pragmatism	Post-positivism	Critical (Post-modernism)	Interpretivism	Interpretivism
Approach	Deductive	Deductive	Deductive/ Abductive	Inductive	Inductive
Strategy	Survey	Survey	Case Study	Case Study	Case Study
Choice	Mono-Method	Mono-Method	Multi-Method	Multi-Method	Multi-Method
Time Horizon	Cross-sectional	Longitudinal	Cross-sectional	Cross-sectional	Cross-sectional
Techniques and Procedures	Questionnaire	Questionnaire	Interviews Structured Literature Review	Interviews Structured Literature Review	Interviews Structured Literature Review

Table 1. Overview of Studies based on Research Onion (adapted from Saunders and colleagues (2007))

Table 1 offers only a first categorization of the underlying worldviews, methods, and applied techniques and procedures. Each study comprises a method section, which provides further details regarding the research assumptions and methodology. Paper A follows pragmatism, since the "research starts with a problem and aims to contribute practical solutions that inform future practice" (Saunders et al., 2007, p. 143) via hypotheses testing. Similarly, Paper B also tests hypotheses in a deductive approach, but, based on the empirical observations, finds that these vary across different contextual settings and, as a result, help to ultimately develop a new understanding.

Whereas Paper A is purely deductive, Paper B and Paper C challenge existing organizational concepts and theories leaning toward abductive reasoning on the basis that extant research might have overlooked important contextual aspects.

Papers C, D, and E comprise both a large-scale case study based on expert interviews as well as several extensive literature reviews. The importance of literature reviews to research is well-established, however, rather young research disciplines such as IS often lack sophistication and appropriateness (e.g., Bandara et al., 2011; Wolfswinkel et al., 2013). Since the literature reviews in the aforementioned papers already produce research findings in and of themselves contributing to theoretical progress and findings, they are considered a standalone method. All papers began with observations, for example, that IT security studies focused mainly on healthcare or financial institutions and rarely accounted for factors influencing decision-making other than economic factors that assumed purely rational decision-makers. Based on this initial observation, and by identifying patterns through data sets (literature analyses and expert interviews), general abstractions are formulated in a bottom-up, or inductive, approach. The majority of the papers are based on a cross-sectional time-horizon—a so-called snapshot of time—

mainly due to time constraints. Paper B measures data from the same sample or cohort at two points in time, not with the intent to measure any change over time but rather to compare the impact of different scenarios on behavioral intention.

In the following chapters, each paper is presented along with the research assumptions and methodology. The chosen research method is explained in further detail, providing more background on the strategies, techniques, and procedures that were applied to achieve relevant research attributions, which are subsequently discussed in Chapter 9.

4 Paper A: Never Change a Running System?

Title

Never Change a Running System? How Status Quo Thinking Can Inhibit Software as a Service Adoption in Organizations

Authors

- Margareta Heidt, Technische Universität Darmstadt, Germany
- Rabea Sonnenschein, Technische Universität Darmstadt, Germany
- André Loske, Technische Universität Darmstadt, Germany

Publication Outlet

Proceedings of the 25th European Conference on Information Systems (ECIS), Guimarães, Portugal. VHB-Ranking: **B**.

Abstract

Despite the "buzz" about Software as a Service (SaaS), decision-makers still often refrain from replacing their existing in-house technologies with innovative IT services. Industry reports indicate that the skeptical attitude of decision-makers stems primarily from a high degree of uncertainty that exists, for example, due to insufficient experience with the new technology, a lack of best practice approaches, and missing lighthouse projects. Whereas previous research is predominantly focused on the advantages of SaaS, behavioral economics conclusively demonstrate that reference points like the evaluation of the incumbent technology or a familiar product are oftentimes prevalent when decisions are made under uncertainty. In this context, Status Quo-Thinking may inhibit decisions in favor of potentially advantageous IT service innovations. Drawing on Prospect Theory and Status Quo Bias research, we derive and empirically test a research model that explicates the influence of the incumbent technology on the evaluation of SaaS. Based on a large-scale empirical study, we demonstrate that the decision-makers' attitude toward SaaS is highly dependent on their current systems and their level of SaaS. A lack of SaaS experience will increase the impact of the Status Quo, thus inhibiting a potential advantageous adoption of the new technology.

Keywords

Status Quo Bias, Prospect Theory, Software as a Service (SaaS), Adoption.

4.1 Introduction

The World Economic Forum stated already in 2010 that "in addition to reducing operational costs, cloud technologies have become the basis for radical business innovation and new business models, and for significant improvements in the effectiveness of anyone using information technology" (World Economic Forum, 2010, p. 1). Fittingly, recent analyses of research institutes forecast the public cloud services market to reach a total of $204 billion in 2016 (e.g., Gartner, 2016; IDC, 2016; Synergy, 2016). A substantial part of that growth is contributed to Software as a Service (SaaS) – the provisioning of applications running on a cloud infrastructure – that will remain the dominant public cloud computing type at an estimated 20.3 percent growth rate resulting in forecasted revenues of roughly $37.7 billion in 2016 (e.g., Cisco, 2016; Gartner, 2016; IDC, 2016). Associated with a large variety of benefits like scalability, mobility or cost savings that are increasingly affirmed by practitioners, SaaS has been hailed as the future default software delivery solution (e.g., Dahlberg et al., 2017). Unsurprisingly, IDC predicts that the penetration of SaaS solutions compared to traditional software deployment will be over 25 percent by 2020 (IDC, 2014). However, especially current European reports show that nearly 80 percent of EU enterprises still do not use cloud services implying that adoption rates are not as high as expected (Eurostat, 2017). Given its role as state-of-the-art technology and innovative service model in an evolving business environment, it is thus crucial to understand why many decision-makers today still refrain from using SaaS in a business environment shaped by increased mobility and disruptive marketing strategies (e.g., Lin & Chen, 2012).

Previous research explains the non-adoption of SaaS in organizations either with legal or strategic requirements to keep data processing completely in-house or as the result of a risk-benefit-analysis (e.g., Benlian & Hess, 2011). Whereas theoretical studies mostly consider purely rational decision-makers, experts claim that decision-makers "have been more protective of their existing infrastructure and, in many cases, have been the biggest obstacle to cloud-based solutions" (van der Meulen & Rivera, 2015). This non-rational behavior is a common assumption in behavioral economics studies when analyzing decisions that are made under uncertainty. Decision-makers actually violate the axioms of rational choice under uncertainty due to cognitive biases or "shortcuts" that compensate for a lack of information or experience (Tversky & Kahneman, 1975). To account for these shortcuts, Kahneman and Tversky (1979) established the so-called Prospect Theory. This theory postulates that people faced with a decision under uncertainty will derive utility from gains and losses measured in relation to some reference points rather than on final assets. The dependence on reference points has been frequently discussed in individual strategic choice contexts and was demonstrated in several empirical studies

on the assessment of new products and services (e.g., Bamberger & Fiegenbaum, 1996; Shoham & Fiegenbaum, 2002). Surprisingly, the SaaS technology adoption literature has largely overlooked this reference-dependence although the decision to adopt SaaS generally entails a high degree of uncertainty due to the unknown complexity of IT security risks, lack of previous experience with cloud-based technologies, or missing best practices and lighthouse projects in the industry (e.g., Eduserv, 2015; Eurostat, 2014; Lin & Chen, 2012). The decision to be protective of their existing (incumbent) infrastructure, i.e., the exaggerated preference for maintaining the current state of affairs, hints at another cognitive bias, namely the influence of Status Quo-Thinking (Samuelson & Zeckhauser, 1988). Status Quo Bias itself has been demonstrated in a wide range of studies of consumer and investment behavior and is increasingly used in management of information systems (MIS) research (Fleischmann et al., 2014). However, research on software selection and particularly studies investigating the intention to adopt cloud-based services did not account for this cognitive bias in decision-making.

To account for this research gap, we first investigated the influence of reference-dependence on SaaS adoption at the organizational level and from there, analyzed how this dependency is affected by Status Quo-Thinking (e.g., Gerlach et al., 2014; Schweitzer, 1995). The distinctiveness of the Status Quo Bias depends on the degree of uncertainty, i.e., the lack of information and experience decision-makers are faced with. Based on the data of a large scale empirical study with decision-makers in charge of the organizational IT, we confirmed our assumptions in a two-step approach: In the first step, we demonstrate the strong influence of the assessment and prevalence of the incumbent in-house technology on decision-makers' attitudes toward a new technology – in our case SaaS. In our second step, we uncover the effect of the Status Quo Bias by comparing experienced and non-experienced or less-experienced decision-makers. We specifically chose SaaS as a clearly definable object of investigation given that the majority of organizations will need to evaluate whether to adopt SaaS as a new technological service model now or in the near future due to the increasing amount of data processing and the demand for mobility (e.g., McLellan, 2016; Rivera & van der Meulen, 2014).

Our study provides several theoretical and practical implications. Given that virtually all technology adoptions nowadays imply a replacement decision, our study highlights the relevance of reference-dependence in MIS research. In this regard, it is essential for future IS research to acknowledge that Status Quo-Thinking has a profound effect on decision-making processes regarding new technology acceptance in organizations. Our findings are also highly relevant to both providers of SaaS and decision-makers of (potential) customer organizations. Providers

should consider the varying degrees of Status Quo-Thinking and group their customers according to their level of SaaS experience. These identified customer groups can be addressed appropriately and more effectively by adapting marketing and sales strategies accordingly, whereas decision-makers need to acknowledge the role of reference points and Status Quo-Thinking to avoid missing out on beneficial technological developments. Joining expert roundtables or including objective assessors could reduce the influence of the Status Quo Bias in decision-making processes. These measures can reduce the possibility that Status Quo-Thinking inhibits SaaS adoption even if the new technology would objectively be the better option.

4.2 Theoretical Background and Hypothesis Development

4.2.1 Technology Adoption Models and Rational Choice

There is a rich tradition in technology acceptance and adoption research. The theories primarily used to study the acceptance and adoption of innovations in information systems or information technologies generally originate in social psychology, such as Theory of Reasoned Action (TRA) (Ajzen & Fishbein, 1980) and its extension Theory of Planned Behavior (TPB) (Ajzen, 1985). Drawing on TRA, many researchers added constructs or derived new models such as Davis' (1986) Technology Acceptance Model (TAM) or Venkatesh et al. (2003) who later consolidated the aforementioned and five further models into the Unified Theory of Acceptance and Use of Technology (UTAUT).

Despite different factors and research model designs, the majority of studies base their assumptions on rational choice, i.e., the rational weighing up of costs and benefits concerning the technology adoption. Specifically, perceived risks and perceived benefits are often singled out and commonly considered as decisive antecedents of behavioral intention or attitude toward SaaS (e.g., Benlian & Hess, 2011) or sometimes described as drivers and inhibitors of SaaS adoption (e.g., Benlian et al., 2009; Lee & Chae, 2013). Several studies look at risks and benefits as relative advantage, i.e., already implicitly weighing up potential benefits of a new technology with the current advantages of the incumbent technology (e.g., Chau, 1996; Wu & Wang, 2005).

In line with the predominant literature stream, we draw on a benefit-risk framework in an organizational setting. Previous research oftentimes studied differences in the perceptions of IT executives' in both SaaS adopter and non-adopter firms, but they did not link the differences they found directly to cognitive biases (Benlian & Hess, 2011). Contrarily, consumer studies went further and high-lighted the importance of reference points as an "anchor" for decisions

to either replace or stick to the incumbent technology or product (e.g., Moqbel & Bartelt, 2015; Roster & Richins, 2009). This dependence on reference points often explains the influence of the incumbent technology when people have to analyze the relative advantage of a new technology during a decision-making process under uncertainty (e.g., Gerlach et al., 2014). Accordingly, it is important to consider Prospect Theory and Status Quo research in the context of organizational SaaS adoption.

4.2.2 Prospect Theory, Status Quo Bias, and Hypotheses Development

Prospect Theory was designed to analyze decision-making processes under uncertainty by considering so-called certainty and isolation effects (Kahneman & Tversky, 1979). These two effects assume that decisions do not necessarily follow mathematical optimality (i.e., the rational weighing up of risks and benefits and their probability weights) due to several reasons: people either underestimate hardly probable outcomes in comparison with certain outcomes and/or people base their decisions rather on change of wealth than on total wealth, i.e., an absolute outcome (Kahneman & Tversky, 1979). Accordingly, Prospect Theory postulates that decision-makers' value functions are rather dependent on reference points than on the actual final outcome. These reference points are defined as the neutral position used by decision-makers in order to determine the extent to which the expected outcomes of a decision constitute gains (i.e., above this position) or losses (i.e., below this position) (Kahneman & Tversky, 1979). Kahneman and Tversky (1984) argue that individuals set up mental accounts to specify advantages and disadvantages associated with the offered option(s) when faced with a transaction or trade decision relative to a certain reference point. Several studies used Prospect Theory to analyze strategic choice and risk/return tradeoffs in organizational decision-making (e.g., Fiegenbaum et al., 1996; Shoham & Fiegenbaum, 2002; Sinha, 1994). It is argued, therefore, that managerial decision processes often depend on reference points because many decisions must be made without advanced knowledge of their full impact and are thereby made under uncertainty. A similar utilization of reference points is at times applied in replacement decisions regarding consumer goods (e.g., Gerlach et al., 2014; Roster & Richins, 2009).

Based on the theoretical underpinnings of Prospect Theory, it can be assumed that a replacement decision in the context of technology adoption generally entails a decision between opting for a new technology or maintaining the incumbent technology, i.e., the enterprise software that is currently hosted and operated in-house on the organization's IT infrastructure. An aggravating factor is the lack of historical data and experiences that inhibits a well-informed, more rational decision-making process. The absence of information or experience is pervasive in the

context of service innovations as lighthouse projects and hard facts about the realization of assumed risks and benefits are missing. To overcome this issue, it can be assumed that the incumbent technology will serve as a reference point for the assessment of a new technology (e.g., Kahneman & Tversky, 1979; Shoham & Fiegenbaum, 2002). Consequently, decision-makers will compare the new technology with the in-cumbent technology because experience and knowledge are available due to the familiarity in this regard. For example, when it comes to the decision whether to replace an existing in-house application with a new SaaS application, we assume that the attitudinal beliefs toward incumbent in-house technologies (i.e., attitudinal beliefs toward the currently used, well-known technology) will serve as reference points for the decision-makers when forming the attitudinal beliefs toward new, yet partly unknown, SaaS technologies. As our research model is based on a risk-benefit framework frequently utilized by previous research in technology adoption (Benlian & Hess, 2011), the attitudinal beliefs are formed by the juxtaposition of perceived benefits and risks. Therefore, the decision-makers perceived benefits of a new SaaS technology will be influenced by the perceived benefits of the incumbent in-house systems that serve as a reference point. Furthermore, decision-makers with little knowledge and experience will tend to underestimate the perceived benefits of SaaS in comparison with their familiar incumbent system. If the level of perceived benefits of the in-cumbent system is high, replacing this system will be regarded as futile. Logically, decision-makers who are fully satisfied with their current in-house system will not regard the potential benefits of a new SaaS solution as equally high. Simultaneously, a decision-maker who perceives the in-house system, for example, as costly and unreliable, will be more prone to change and will not consider this deviation from a certain outcome (i.e., subsequent use of the incumbent system) as a loss. Accordingly, decision-makers who perceive the risks of their incumbent system as high, are more likely to consider a new SaaS technology to be less risky. Therefore, we hypothesize:

> ***H1a**. Perceived benefits of in-house systems are negatively associated with the decision-makers' perceived benefits of SaaS.*

Analogously, we assume the same influence regarding the evaluation and reference-dependence of the perceived risks:

> ***H1b**. Perceived risks of in-house systems are negatively associated with the decision-makers' perceived risks of SaaS.*

The benefits and risks associated with a new technology are fundamental in technology adoption decisions. Thus, previous studies in SaaS adoption show that behavior and intentions are

largely determined by weighing up risks and benefits (e.g., Benlian & Hess, 2011). These overall perceived risks and benefits include financial, strategic, security, performance, and management dimensions (Benlian & Hess, 2011). In line with previous SaaS research (e.g., Benlian & Hess, 2010, 2011; Lee, 2009), we expect perceived risks to generally have a negative impact on decision-makers' intentions to adopt a SaaS technology. For example, if decision-makers perceive a high risk of downtime errors and data loss to be associated with SaaS technologies, they will be less likely to consider an adoption of this new SaaS technology. On the other hand, the perceived benefits are generally expected to positively influence decision-makers' intentions to adopt. For example, if decision-makers perceive SaaS technologies to be associated with potential cost reductions (e.g., due to lower server administration costs) their intention to adopt SaaS will be positively influenced. There-fore, high perceived benefits will more likely lead to an intention to adopt, whereas the perceived risks of SaaS will inhibit the intention to adopt. Accordingly, we further hypothesize:

> ***H2a.****: Perceived benefits of SaaS are positively associated with the decision-makers' intention to adopt SaaS.*
>
> ***H2b.*** *Perceived risks of SaaS are negatively associated with the decision-makers' intention to adopt SaaS.*

Building on Prospect Theory and several experiments, Tversky and Kahneman (1985) discovered that decision-makers prefer to be passive and inactive rather than experiencing negative results due to their actions or decisions. Some literature refers to this concept as reference point bias (Levy, 1997) whereas a more common stream of research coined the term Status Quo Bias as an effect of the loss aversion discussed in Prospect Theory (Kahneman et al., 1991; Samuelson & Zeckhauser, 1988). Loss aversion entails an overestimation of certain positive outcomes, whereas potential losses are weighted disproportionately. This demonstrates the preference for the current state of affairs, i.e., if individuals take the Status Quo as a reference point, then they will perceive any deviation from it as loss. Therefore, a decision-maker will avoid change and an unknown outcome unless the advantages clearly outweigh the perceived disadvantages. Another explanation for the Status Quo Bias is provided by Zajonc (1968) and Bornstein (1989) who argue that mere exposure to a stimulus (i.e., the incumbent product) enhances the attitude toward it and, therefore, argue that familiarity leads to liking.

A well-known example for the maintenance of the Status Quo is the QWERTY keyboard. Although a different arrangement of letters could lead to a more productive and better keyboard, QWERTY is still omnipresent because switching from the Status Quo could entail huge costs

of retraining individuals and replacing the current design in systems and devices (David, 1985). Especially, research on replacement decisions regarding (technological) consumer goods consider these high potential switching costs to inhibit a change from the Status (e.g., Moqbel & Bartelt, 2015; Roster & Richins, 2009). Studies focusing on technology systems are increasingly building on these findings adding further contributing factors like habit or inertia (e.g., Kim & Kankanhalli, 2009; Polites & Karahanna, 2012). Almost all of these studies attribute the Status Quo Bias at least partially to in-sufficient available information and experience. Past experiences serve as an "anchor" or "frame" for decisions as decision-makers frequently do not exclusively follow rational concepts of mathematical optimality (Schwenk, 1984; Slovic, 1975).

In line with previous research, we expect that decision-makers in companies that already possess a certain degree of knowledge and past experience will demonstrate a lower Status Quo Bias in comparison to less or non-experienced decision-makers. Decision-makers with a low level of SaaS experience, will be more affected by the Status Quo Bias because they overestimate the losses that they would encounter when replacing the incumbent technology. Therefore, the correlation postulated in hypotheses H1a and H1b will be increased. On the other hand, decision-makers who already possess a SaaS solution among their incumbent in-house technology will draw on the experience that they already accumulated with SaaS. Therefore, their decision-making process will be better informed and consequently less affected by Status Quo-Thinking. Greater experience and further facts available to decision-makers will enable a more "rational" decision-making process (Bazerman, 2008). For example, experienced decision-makers can judge the perceived benefits like cost reductions without drawing upon a comparison to their incumbent system because a previous adoption of a SaaS technology already proved to be cost-efficient. Similarly, experienced decision-makers will evaluate the perceived risks of SaaS depending on past experience and be less affected by Status Quo Bias. Whereas, inexperienced decision-makers might, for example, believe that downtime issues are more pronounced in contrast to their reliable in-house technology and will thus attribute higher perceived risks to a new SaaS technology. Hence, we hypothesize:

> ***H3a**. Perceived benefits of in-house systems will have a stronger negative association with the perceived benefits of SaaS for organizations with no or low SaaS experience than for organizations with SaaS experience.*

H3b. *Perceived risks of in-house systems will have a stronger negative association with the perceived risks of SaaS for organizations with no or low SaaS experience than for organizations with SaaS experience.*

The research model is shown in Figure 1.

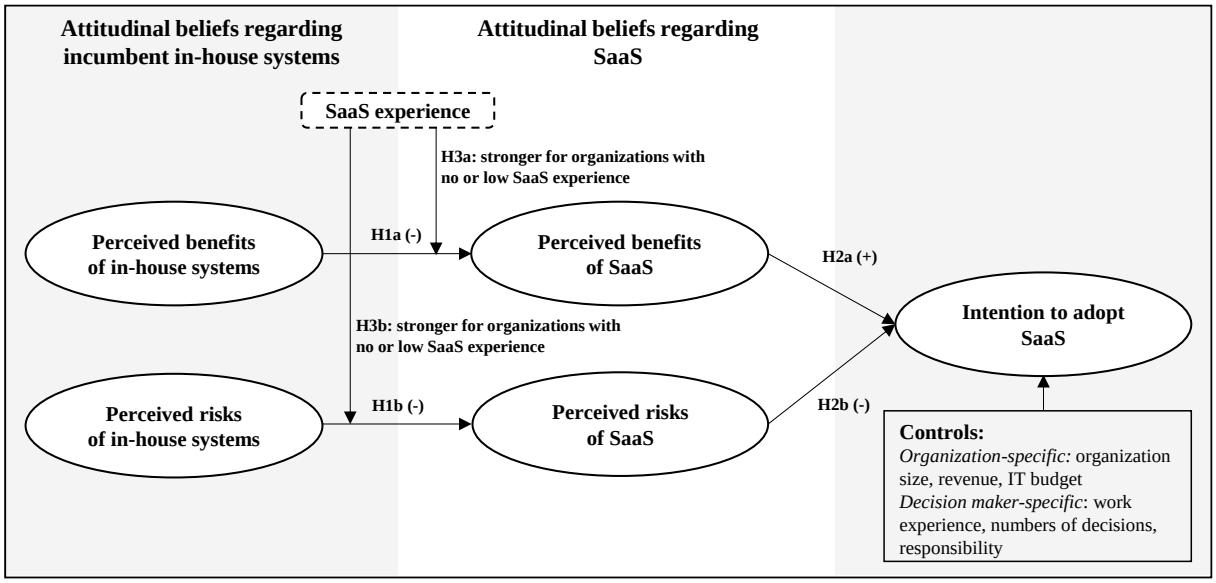

Figure 6. Research Model

4.3 Research Methodology and Data Analysis

4.3.1 Survey Administration and Sample Characteristics

Construct validity was established by adopting validated measurement items from previous research studies with minor changes in wording. All latent constructs were reflective and measured with multiple items on a 7-point Likert scale. To ensure a consistent understanding of enterprise software in case of in-house systems and in case of SaaS, we used the following definitions within the study:

- **Enterprise software** is defined as business applications, such as Customer Relationship Management (CRM) systems, Enterprise Resource Planning (ERP) systems, or Project Management (PM) applications.
- **SaaS** is defined as enterprise software provided by a supplier and accessible via a public network, such as the Internet (i.e., public cloud).
- **In-house systems** are defined as enterprise software that is hosted and operated on the organization's IT infrastructure.

As suggested by previous research, we included work experience (in years), numbers of sourcing decisions already made, the responsibility for sourcing decisions in the organization (1=not responsible at all - 4=completely responsible), organization size (revenue and number of employees), and IT budget as controls in our research model (Benlian, 2009; Hsu et al., 2015). We pre-validated our measurement model in a pretest with 8 MIS researchers by using a cognitive interview technique. The pretest resulted in minor changes to improve the clarity of the model. Our study's final measurement items are shown in Table 1.

Constructs	Items	Source
Perceived risks	How do you evaluate the overall risk (i.e., financial, strategic, security, performance, and management risks) associated with adoption of [in-house / SaaS] applications? (1=not risky at all - 7=extremely risky)	Based on Featherman and Pavlou (2003)
	How do you evaluate the risk that the expected benefits of adopting [in-house / SaaS] applications will not materialize? (1=not risky at all - 7=extremely risky)	
	How do you evaluate the danger that is generally associated with the adoption of [in-house / SaaS] applications? (1=not risky at all - 7=extremely risky)	
Perceived benefits	The overall advantage of adopting [In House / SaaS] applications is… (1=very low - 7=extremely high)	Based on Gewald and Dibbern (2009)
	The potential cost reduction associated with the adoption of [in-house / SaaS] applications is... (1=very low - 7=extremely high)	
	Overall, I consider [in-house / SaaS] adoption to be a useful strategic option. (1=strongly disagree - 7=strongly agree)	
Intention	If there is a superior offer, a SaaS solution should be used for the application domain that I am in charge of. (1=strongly disagree - 7=strongly agree)	Based on Gewald and Dibbern (2009)
	Our company should increase the existing level of adopting SaaS applications. (1=strongly disagree - 7=strongly agree)	
	I support the further adoption of SaaS applications for the application domain that I am in charge of. (1=strongly disagree - 7=strongly agree)	

Table 2. Overview of Constructs

Our quantitative study was conducted between March 17 and May 1, 2016 in a European country. In a key informant approach, we contacted a total of 1,126 decision-makers from organizations of various industries via a contact request on an online social business network. To encourage participation, a management report about the results was offered to the participants. A total of 251 (22.3%) of the 1,126 contacted decision-makers agreed to participate in our study and were sent links to access the online survey. One week after sending the invitation, a reminder was sent via another direct message on the social business network. With 131 completed surveys, the response rate was 11.6%. Two main reasons were given for not participating: the contacted decision-makers either stated time pressure or that their organizations do not participate in such studies in general. Altogether, 4 of the 131 participants stated to be not responsible for sourcing decisions in their organizations and 4 data sets were identified to have poor data

quality. These 8 data sets were excluded from the data analysis, which is therefore based on 123 valid data sets. The sample characteristics can be extracted from the following Table 2.

Company size (number of employees)		**Position**	
Small (<50)	36 (29.3%)	CEO	3 (2.4%)
Medium (50-249)	18 (14.6%)	CIO	73 (59.3%)
Corporation (>249)	69 (56.1%)	CTO	20 (16.3%)
Sales p.a.		IT Manager	21 (17.1%)
<1 m EUR	22 (17.9%)	Others	6 (4.9%)
1-9 m EUR	23 (18.7%)	**Work experience**	
10-99 m EUR	23 (18.7%)	1-5 years	16 (13.0%)
>99 m EUR	55 (44.7%)	6-10 years	30 (24.4%)
		11 years and more	77 (62.6%)

Table 3. Overview of Sample Characteristics

In addition to these sample characteristics, we further analyzed the differences within our sample according to the proportion of participating industry sectors and the respective average level of SaaS experience within those sectors. Table 3 shows the proportion of each industry sector relative to the overall sample and the average level of self-reported SaaS experience in each industry (0%=complete absence of SaaS use-100%=all enterprise applications deployed as a service). According to our analysis, most respondents work in IT, Professional Services, and Manufacturing and the highest experience levels are reported by decision-makers in Telecommunications, IT, Retail, and Professional Services.

Industry sector	**Proportion of total sample**	**Average SaaS experience**
Real Estate	0.8%	0 %
Travel & Tourism	0.8%	0 %
Education & Administration	4.1%	1.20 %
Pharmacology & Medical	2.4%	3.33 %
Logistics & Transportation	3.3%	3.75 %
Energy & Utilities	2.4%	5.00 %
Health Care	4.1%	7.00 %
Manufacturing	13.0%	7.06 %
Construction	5.7%	7.14 %
Consumer Goods	2.4%	8.33 %
Financial Services	6.5%	27.00 %
Professional Services	17.1%	34.43 %
Retail & Wholesale	6.5%	37.00 %
Information Technology (IT)	22.8%	39.00 %
Telecommunications	4.9%	53.33 %
others	3.3%	33.75 %

Table 4. Segmentation of Industry Sectors

4.3.2 Assessment of Measurement Validations

The Shapiro-Wilk Test showed that the data is not normally distributed. Furthermore, we calculated the time to respond by considering the number of days between sending access to the online survey to the participants and the actual survey completion to test for non-response bias. Based on that, we compared the data of the first 25% of participants (i.e., shortest time to respond in days) with the last 25% (i.e., longest time to respond in days) (Armstrong & Overton, 1977). The Mann-Whitney-U test revealed the non-existence of significant differences. Given that studies using self-report measures to capture dependent and independent variables in the same survey might suffer from common method biases (Podsakoff et al., 2003), we included a marker variable in our survey. The results of the correlation analysis did not indicate significant correlation between the marker variable and the measurement variables. Accordingly, it can be assumed that our data does not suffer from common method bias (Lindell & Whitney, 2001).

Due to the explorative nature of our study and the non-normality of our data, we evaluated our research model by using the non-parametric Partial Least Squares (PLS) methodology following the guidelines proposed by Hair et al. (2013). Correspondingly, we first evaluated criteria for discriminant and convergent validity in order to assess our measurement model correctly. Therefore, we extracted parameters for indicator reliability, composite reliability (CR), average variance extracted (AVE) and computed Cronbach's alphas (CA) (see Table 4). With a single exception (indicator 2 of perceived benefits: 0.655), all outer loadings are above the threshold of 0.7. However, all indicator reliability values are larger than the minimum acceptable level of 0.4 and beyond that, most of them are close or above the optimal level of 0.7 (Hulland, 1999). The values of composite reliability of all constructs are well-above the threshold level of 0.7, as suggested by Bagozzi and Yi (1988). Regarding AVE, the values of all the constructs exceed the level of 0.5 (Bagozzi & Yi, 1988) and the values for Cronbach's alpha, reflecting the internal consistency of the constructs, are also all above the threshold of 0.7 (Nunnally, 1978). Moreover, according to Hair et al. (2012)'s recommendation of sample sizes in PLS, a statistical power of 80% is sufficient for a measurement model with a sample size of 123. In summary, the discriminant and convergent validity of our model can be presumed.

#	Construct	Loadings	Indicator reliability	CA	CR	Correlation to Construct # / Square root of AVE [bold]				
						1	2	3	4	5
1	Risks in-house	0.864-0.936	0.746-0.876	0.886	0.929	**0.902**				
2	Risks SaaS	0.800-0.881	0.640-0.776	0.814	0.888	-0.540	**0.852**			
3	Benefits in-house	0.706-0.858	0.498-0.736	0.704	0.832	-0.488	0.534	**0.790**		
4	Benefits SaaS	0.655-0.897	0.429-0.805	0.742	0.850	0.471	-0.605	-0.439	**0.811**	
5	Intention SaaS	0.885-0.960	0.783-0.904	0.925	0.952	0.540	-0.727	-0.522	0.720	**0.932**

Table 5. Assessment of Measure Models

The Fornell-Larcker Criterion Analysis for checking discriminant (Fornell & Larcker, 1981) showed that the square root of the AVEs of each construct (highlighted bold) is greater than the correlations among the construct with any other construct in the model (see Table 4). In sum, it can be concluded that our measurement model is well-specified.

To test for multicollinearity, we calculated the Variance Inflation Factor (VIF) values. The VIFs values (Risks in-house=1.313, Risks SaaS=1.903, Benefits in-house=1.313, Benefits SaaS=1.749) are all below 5 (Hair et al., 2011). Thus, we can exclude collinearity problems for our model.

4.3.3 Data Analysis and Results

In order to test our hypotheses, we chose a two-step data analysis approach (see Figure 2). In the first step, we test our research model regarding the influence of reference points (attitudinal beliefs about incumbent in-house systems) on the perception of risks and benefits associated with SaaS (attitudinal beliefs about SaaS) (H1a and H1b) as well as the resulting intention to adopt SaaS (H2a and H2b). In the second step, we utilized a multi-group analysis (MGA) for analyzing whether the influence of reference points is moderated by the existing experience with SaaS applications.

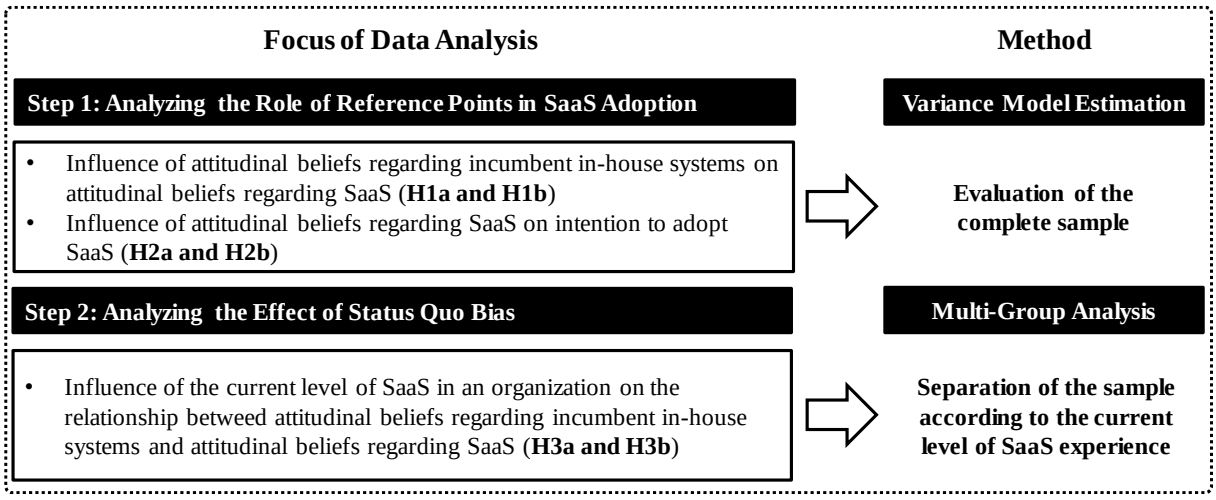

Figure 7. Data Analysis

4.3.3.1 Step 1: The Role of Reference Points in SaaS Adoption

To test our hypotheses H1a and H1b as well as H2a and H2b, the effect sizes and significance of path coefficients were evaluated based on a PLS algorithm and a bootstrapping procedure (5,000 samples, no sign change option, mean replacement). The results are shown in Table 5.

We found that the perceived benefits of in-house systems are significantly negatively associated with the perceived benefits of SaaS (β=-0.451, $p<0.001$), supporting H1a. The negative relationship between the perceived risks of in-house systems and perceived risks of SaaS is also identified to be significant (β=-0.545, $p<0.001$), supporting H1b. Regarding H2a we found that the positive association of perceived benefits of SaaS with the intention to adopt SaaS is significant (β=0.439, $p<0.001$). Thus, H2a is supported. Moreover, our analysis showed that the negative association of the perceived risks of SaaS with the intention to adopt SaaS is significant (β=-0.462, $p<0.001$). Accordingly, H2b is supported as well.

Following the bootstrapping-based approach of Preacher and Hayes (2008), we found that a significant indirect effect of the perceived benefits of in-house systems on the intention to adopt SaaS through the perceived benefits of SaaS is -0.198 (p=0.006). The size of the indirect effect of the perceived risks of in-house systems on intention to adopt SaaS through the perceived risks of SaaS is significant with an indirect effect size of 0.252 (p=0.002).

In sum, the results show that our model explains 70.2% of variance in the intention to adopt SaaS (R^2=0.702), 29.7% of the variance in perceived benefits of SaaS (R^2=0.297), and 20.3% of the variance in the perceived risks of SaaS (R^2=0.203).

Relationship	Path coefficients	Results
Perceived benefits of in-house systems → perceived benefits of SaaS	-0.451***	*H1a supported*
Perceived risks of in-house systems → perceived risks of SaaS	-0.545***	*H1b supported*
Perceived benefits of SaaS → intention to adopt SaaS level	0.439***	*H2a supported*
Perceived risks of SaaS → intention to adopt SaaS	-0.462***	*H2b supported*
Significance level: ***p < 0.001		

Table 6. Results of the Variance Model Estimation

There was no significant influence of the control variables (work experience: β=0.059, p=0.427; number of decisions: β=0.009, p=0.722; self-stated responsibility for sourcing decisions: β=-0.021, p=0.512; revenue: β=0.025, p=0.598; size: β=-0.031, p=0.477; IT budget: β=0.069, p=0.439).

4.3.3.2 Step 2: The Effect of Status Quo Bias on Attitudinal Beliefs Regarding SaaS

In order to test H3a and H3b, we had to perform a multi-group analysis (MGA) procedure (e.g., Hair et al., 2011; Sarstedt et al., 2011). Accordingly, we separated our data set into two groups: organizations currently maintaining almost all of their enterprise applications in-house (i.e., organizations with no or a low SaaS level) and organizations that already utilize a substantial degree of SaaS (i.e., organizations with a medium or high SaaS level). We split the data sets at a marginal level of SaaS use of 5% in an organization. Accordingly, organizations that still host more than 95% of their enterprise applications in-house (n=39) are considered to have less experience with the new technology, thus, face a higher level of uncertainty when making decisions about future SaaS usage. On the other hand, organizations that already use 5% or more of their enterprise applications as a service (n=84) are assigned to the group that is expected to have a certain degree of experience with SaaS and, therefore, will base the adoption decision less on reference points (attitudinal beliefs about in-house systems). The results of the MGA are shown in Table 6. These results show that all of the hypothesized relationships in H1 and H2 are significant for both organizations with no or low SaaS experience and organizations with medium or high SaaS experience. However, the path coefficients of the relationships between perceived benefits and risks of in-house systems and perceived benefits and risks of SaaS are found to be significantly different with respect to the differences in experience with SaaS. Specifically, the negative influence of perceived benefits of in-house systems on the perceived benefits of SaaS is significantly higher for organizations that have no or low SaaS experience (β=-0.640; p<0.001) than for organizations that have medium or high SaaS experience (β=-0.379; p=0.008; MGA p=0.029). Accordingly, H3a is supported. Regarding the relationship

between the perceived risks of in-house systems and perceived risks of SaaS, significant differences were found as well (MGA p=0.017). As such, the negative relationship between the perceived risks of in-house systems and perceived risks of SaaS is significantly higher for organizations with no or low experience with SaaS (β=-0.728; p<0.001) than for organizations with a medium or high level of experience with SaaS (β=-0.445; p=0.001). Therefore, H3b is supported. Differences between the two groups of organizations regarding the influence of perceived benefits and risks of SaaS on the intention to adopt SaaS were not found.

Relationship	**Path coefficients**		**p-value of Multi-Group Analysis**	**Results**
	Low or no SaaS experience (n=39)	**Medium or high SaaS experience** (n=84)		
Perceived benefits of in-house systems → perceived benefits of SaaS	-0.640***	-0.379***	0.029	*H3a supported*: stronger for organizations with no or low SaaS experience
Perceived risks of in-house systems → perceived risks of SaaS	-0.728***	-0.445***	0.017	*H3b supported*: stronger for organizations with no or low SaaS experience
Significance level: ***p < 0.001				

Table 7. Results of the Multi-Group Analysis

4.4 Discussion

Previous research has repeatedly highlighted the importance of perceived risks and benefits in organizational service innovation adoption (e.g., Benlian & Hess, 2011; Featherman & Pavlou, 2003; Wu et al., 2011). However, when analyzing decisions about replacing incumbent technologies with new technologies, it is essential to consider the complexity along with the high degree of uncertainty due to a lack of experience surrounding such decisions. Confronted with decision-making under uncertainty, individuals often rely on cognitive "shortcuts", i.e., the dependence on reference points in a particular decision-making process (Shoham & Fiegenbaum, 2002). In the context of a replacement decision of an existing in-house technology with a new technology, decision-makers encounter a lack of information because of lacking experience or absent historical data that induces such cognitive shortcuts. On account of this, we developed a research model that demonstrates the influence of incumbent technologies (i.e., in-house systems) on the assessment of attitudinal beliefs (i.e., perceived benefits and risks) regarding SaaS on the basis of Prospect Theory and Status Quo Bias research. In a two-step analysis, based on the data of a large scale empirical study with decision-makers who are responsible for the organizational IT, we (1) identified the significant influence of reference-dependence affecting the rational weighing up of risks and benefits associated with a new SaaS technology and (2)

measured the effect of the Status Quo Bias depending on the already ac-quired experience level of SaaS use.

We discovered that decision-makers' assessments of a new SaaS technology are negatively influenced by their attitude toward the incumbent technology. In other words, if decision-makers consider their incumbent system to be satisfactory because the perceived benefits outweigh the perceived risks, they will tend to form a rather negative attitude toward new, unfamiliar SaaS technologies. Vice versa, decision-makers that, for example, already experienced security incidents with their in-cumbent technology and thus perceive higher risks associated with existing in-house solutions, will more likely display a positive attitude toward SaaS. Accordingly, decision-makers who realized that their incumbent system does not offer financial benefits (any longer) will be more receptive of potential cost reductions offered by a SaaS solution and therefore, perceive benefits of SaaS higher. To conclude, the incumbent technology can exert a pronounced influence on the final SaaS adoption decision.

In addition, our results illustrate that the dependence on reference points differs significantly according to the SaaS experience in the respective organization. In contrast to previous research (Vetter et al., 2011) we are not measuring self-stated experience with SaaS according to Dibbern (2004) or Roodhooft and Warlop (1999), but rather control our study for this relationship with a defined moderator variable called SaaS experience for objective measurement. We were able to demonstrate a stronger influence of the Status Quo Bias in organizations with little to no SaaS experience. Especially, less experienced decision-makers will regard the retention of the Status Quo as less risky compared to the potentially negative consequences of an adoption or replacement decision. This in-accurate assessment of risks can be regarded as a result of loss aversion, i.e., the overestimation of perceived risks of the SaaS solution. For example, decision-makers could overestimate the probability and the actual consequences of down-time issues and will assess this risk more severely compared to the current risks of their incumbent system. Thus, without the necessary knowledge and past experience, a deviation from the incumbent system will be regarded as an unnecessary risk resulting in the retention of the Status Quo.

Our study offers several theoretical and practical implications. We specifically contribute to the stream of technology acceptance research by singling out the importance of reference points and Status Quo Bias in the context of SaaS adoption decisions. In particular, our study is the first using Prospect Theory to analyze decision-makers' appraisals of SaaS in an organizational context by considering their evaluation of the incumbent technology they are familiar with. Moreover, our results indicate that Status Quo-Thinking is more pronounced according to the

experience level indicating that adoption decisions of service innovations are potentially more affected by Status Quo Bias. Given that new organizational IT systems are almost exclusively replacement decisions, future research should consider the relevance of incumbent systems when devising their study designs. We deliberately chose a research approach based on a very generic risk-benefit assessment which could thus be adjusted according to other scenarios considering adoption, service innovation, or replacement decisions (Lee, 1999). In addition, our way of measuring the Status Quo Bias at the group level can con-tribute to future research as most studies so far measure Status Quo Bias with indicators such as perceived inertia or perceived sunk costs that are predominantly based on self-assessment on an individual level (e.g., Polites & Karahanna, 2012).

We also offer insights and contributions for practice. Our results indicate that providers of SaaS technologies need to adapt their business models by altering their communication and sales approach according to the respective group of potential customers. Customer groups which already passed a certain threshold in terms of their SaaS level, suffer from a less pronounced degree of Status Quo Bias and will, therefore, be easier to convince of the relative advantage of SaaS and potentially display a higher intention to adopt further solutions. Hence, providers should intend to further capitalize on their current client base with additional horizontal or vertical integration solutions. Another approach for providers that involves the current client base is customer recommendation programs. Due to the social influence on risk assessment (Lee, 1999), recommendations given by existing customers can decrease the level of uncertainty. Especially, non-adopters will demand more facts and examples to realize the relative advantage of a SaaS solution and, therefore, organized roundtables with SaaS-experienced organizations can help both SaaS providers and unexperienced decision-makers to realize financial or strategic advantages. A similar way to decrease the inherent Status Quo Bias is the acquirement of further knowledge gained in workshops, lighthouse projects or extended trial versions to gain more experience with a potential new technology. From an organizational perspective, decision-makers can already benefit from our study by acknowledging the in-fluence of reference points and Status Quo-Thinking. In order to arrive at a more objective assessment of risks and benefits of both the incumbent and new technology, organizations should, therefore, encourage roundtables or group discussions. These decision-making processes should also include objective assessors such as consultants to accomplish a more objective and rational evaluation of both their incumbent system as well as a possible new SaaS solution. Furthermore, decision-makers might be unaware of the difficulties their employees experience with the incumbent technology and, as a consequence, overestimate the benefits of the existing systems. This may

result in a distorted perception of the new technology and, hence, obstruct an optimal adoption or replacement decision. Additional information from various parties in the organizational hierarchy might compensate for this lack of information and support an optimal decision-making process further. Against this backdrop, organizations should also scrutinize if their current company culture might encourage Status Quo-Thinking. Previous research in this context demonstrated that company culture itself can enhance Status Quo-Thinking when decision-makers "reflect the imprint of cultural socialization more so than professional experience" (Geletkanycz, 1997, p. 615). According to Geletkanycz and Black (2001), a deviation from the Status Quo will be regarded even more as an unnecessary risk that could possibly jeopardize a decision-maker's position in those organizations characterized by more hierarchical and traditional cultures. Interestingly, our descriptive analysis indicates indeed that more "traditional" industry sectors seem to be less likely to adopt SaaS. Consequently, organizations and individual decision-makers should realize that the Status Quo Bias might actually be an obstacle for achieving certain organizational goals, and therefore encourage processes and measures that minimize Status Quo-Thinking.

4.5 Limitations, Future Research, and Conclusion

As with any research, some limitations of this study merit consideration. First, our study is cross-sectional and static. IT services and systems constantly change entailing new requirements and the perceptions of new as well as incumbent technologies might change over time. As such, future re-search could enrich the findings of our study regarding the replacement process by measuring the assessments of different technologies longitudinally. By doing so, factors that address the Status Quo Bias, and especially factors that could quickly change the attitude toward the new technology, could be identified in order to develop appropriate countermeasures. Second, this study focuses on the top echelon's assessments of incumbent and new technologies. Even if these decision-makers are ultimately responsible for the sourcing decisions in their organizations, IT decisions are often made by groups and may also be influenced by other organizational stakeholders (e.g., customers or investors). Future research can supplement our results by conducting case studies and expert interviews with decision-makers at different hierarchical levels in order to fully capture the technology re-placement process in organizations. In addition, the results of this study need to be verified within the context of other decisions about organizational technology adoption and in different cultural and legal settings. Decision-makers in US companies or in more traditional industry sectors might dis-play different perceptions and attitudes or draw on different reference points due to divergent company cultures

than those in Europe, Asia or innovative and service-oriented industries. By way of example, a future study directed primarily at start-ups that are faced with green-field adoptions could analyze whether the attitude toward SaaS is influenced by different reference points (e.g., experience with a technology in a previous organization or recent news about security breaches). Another recommendation for future research would, therefore, encompass experiments to verify our results and to test for other effects, such as further cognitive biases in the organizational decision-making process.

To sum up, our study enhances the understanding of an organization's acceptance of SaaS technologies in particular and replacement decisions in general. When decision-makers are confronted with a new technology, they frequently encounter a lack or insufficiency of data and experience. As this is often the case when assessing SaaS technologies, decision-makers will draw on their experience with familiar technologies and evaluate the new technology based on their assessment of the existing one. It is essential for SaaS providers to acknowledge this relationship as they risk losing potential selling opportunities if they neglect to frame their sales strategy and marketing efforts according to these cognitive decision-making processes. Correspondingly, decision-makers in organizations should be aware that their assessments of risks and the benefits associated with the incumbent technology may be skewed due to Status Quo-Thinking, which in turn, may discourage their organizations from adopting a more efficient technology and inhibiting service innovations in general. Neglecting to acknowledge these findings could have far-reaching negative consequences for overall organizational performance.

5 Paper B: To (Psychologically) Own Data is to Protect Data

Title

To (Psychologically) Own Data is to Protect Data: How Psychological Ownership Determines Protective Behavior in a Work and Private Context.

Authors

- Margareta Heidt, Technische Universität Darmstadt, Germany
- Christian M. Olt, Technische Universität Darmstadt, Germany
- Peter Buxmann, Technische Universität Darmstadt, Germany

Publication Outlet

Internationale Tagung der Wirtschaftsinformatik (WI), Siegen, Germany. VHB-Ranking: **C.**

Abstract

The ever-rising rates of data generation entail new opportunities for business and society but also an increasing risk of data breaches. Apart from technical measures, approaches like password authentication to ensure data protection revolve around the end-user as the human element in information security. Drawing on organizational research which argues that the sole feeling of ownership towards an intangible target like data can lead to heightened levels of the individual's responsibility, we investigate whether and to what extent this ownership feeling differs between personal files and data accessed in the work context. To this end, we draw on data derived through a two-phase questionnaire among a representative group of 209 employees. Consequently, we find evidence that psychological ownership shows stronger effects on protection motivation among participants in a private context. Furthermore, results indicate that employees partly relinquish their responsibility regarding security responses to protect data in their work context.

Keywords

Password Security, Psychological Ownership, Employee, Home User, Protection Motivation Theory

5.1 Introduction

According to the latest estimations in 2012, 2.7 million terabytes existed in the digital universe with roughly 35 zettabytes of data generated annually by 2020 (IBM, 2012). Data generation is

further fueled through the acceleration of the Internet of Things and the growth of worldwide internet users to 4 billion in 2018 (Statista 2018).

Unsurprisingly, the age of big data promises new opportunities for business and everyday life but entails new flip sides as evidenced by the ever-increasing frequency and amount of damage of data breaches by cyber criminals. Verizon's annual report estimates that 81 percent of data breaches that occurred since 2014 were caused by stolen or weak passwords (Verizon, 2018). An estimation particularly striking as the most prevalent approach to both access and protect private and business data remains through password authentication. Passwords can thus be considered a particular vulnerability as they are especially intertwined with the human element in information systems – the end-user. Since end-users have been continuously identified as the "weakest link" within the security chain, behavioral information security research emerged as an important subfield of information systems (IS) (e.g., Crossler et al., 2013; Schneier, 2000).

Human behavior in IS security has been drawing on psychology, criminology or health science and various adapted frameworks and models have been applied numerously within the end-user context, examining either employee or individual private user behavior (e.g., Crossler et al., 2013; Lebek et al., 2014; Mayer et al., 2017). These models show that factors such as the certainty of sanctions, the risk appraisal of a cyber threat or perceived behavioral control are strong indicators leading to the behavioral intention to perform certain protective actions (e.g., Boss et al., 2015; Bulgurcu et al., 2010). However, extant studies have only identified and analyzed the effectiveness of these factors on security in *either* a work environment *or* in the context of private use (Mou et al., 2017). Thus, it remains unclear if certain factors affect the intention to behave in a more secure way in order to protect - one's own or the company's – data even though context-sensitivity of findings has recently received increased attention among IS scholars (Davison & Martinsons, 2016).

In this regard, existing studies (e.g., Anderson & Agarwal, 2010; Menard et al., 2018) have suggested that the sole feeling of possession or "being psychologically tied to an object" (Pierce et al., 2001) might lead to heightened levels of individual responsibility and engagement in IS security behavior. This feeling is referred to as "*psychological ownership*", a concept that describes the self-derived perception of ownership opposed to the actual legal ownership which is backed by the perception of others and the legal system. Psychological ownership (PO) is rooted within the innate human need to experience possession of either tangible or intangible targets (Duncan, 1981) and the sense of regarding this target as extension of one's self (Dittmar,

1992). In turn, human desire to experience control and accountability over the target differs according to the level of PO the individual experiences (Furby, 1978; Pierce et al., 2001).

However, IS studies thus far have either focused on feelings of ownership towards the targets 'internet' or 'one's computer' among home-users (Anderson & Agarwal, 2010) or towards the target 'information' in a generic work-based scenario (Menard et al., 2018). Whereas the first study argues for a direct influence of PO on intention to protect the target of ownership, the latter theorizes how PO affects the protection motivation, i.e., antecedents of intention to protect information. Again, both of the aforementioned studies and others that integrated PO into the privacy calculus (Cichy et al., 2014) or explored PO of IT (Klesel et al., 2016), have only examined the role of PO in one single context and have not questioned yet how levels of PO might differ according to situational differences in contexts. But do individuals really experience the same degree of PO regarding, for example, their own electronic device or one provided through their company? Or do individuals experience higher levels of PO regarding their personal data as opposed to PO regarding the data they work with – and are supposed to protect through appropriate security measures – in their professional environment?

Against this backdrop, we seek to (1) extend prior research on individuals' protection motivation of data by highlighting the distinct role of PO in both a work and a private context. Furthermore, our study is the first to our knowledge that actually (2) compares protection motivation based on a longitudinal study and one distinct sample in both contexts.

The remainder of this article is structured as follows: the theoretical background of both Protection Motivation Theory and psychological ownership is presented and serves as the foundation of our hypotheses which are integrated into a research model and tested in both a work and private setting. Subsequently, the results of our study are demonstrated and discussed before implications for theory and practice are derived

5.2 Theoretical Background and Hypotheses Development

The following section provides an overview of the current state of behavioral IS security research in both work and private contexts along with the basics of the aforementioned concept of psychological ownership and how it has been accounted for thus far in IS security literature. Based on the theoretical background, hypotheses are developed and integrated into our research model which draws on Protection Motivation Theory (PMT).

5.2.1 Information Security Research

IS research has a long-standing tradition of analyzing security-related issues on an organizational and individual level (Liang & Xue, 2010; Straub & Welke, 1998). In an organizational context, researchers continue to advance technical approaches to prevent intrusion or to detect attacks (Cavusoglu et al., 2009; Hansen et al., 2007), however behavioral information security research has gained considerable momentum during the last two decades by focusing on human, and in particular, end-user behavior in work and private use contexts.

Within behavioral information security research, users can generally be divided into two subgroups in a work context: users that exhibit deviant behavior, i.e., compromising information security through espionage, theft, or sabotage, and those users who misbehave without the intent to cause damage (Willison & Warkentin, 2013). By means of example, the latter group's misbehavior can manifest itself through defiance of security policy aspects such as using corporate devices to access non-work-related websites or utilizing weak, repetitive and thus easy-to-compromise passwords for important work accounts (Herath & Rao, 2009). In order to understand the driving factors of such "unintended" misbehavior or to identify aspects that encourage the use of safeguarding practices, IS researchers have heavily relied on behavioral theories that originate in behavioral psychology, organizational science, criminology, or health research (e.g., Anderson & Agarwal, 2010; Boss et al., 2015; Bulgurcu et al., 2010; Lebek et al., 2014; Mayer et al., 2017).

Protection Motivation Theory has been widely used to analyze "any threat for which there is an effective recommended response that can be carried out by the individual" (Floyd et al., 2000, p. 409) and thus serves as a widespread theory in IS security research due to its applicability to security threats such as violating security compliances (Pahnila et al., 2007) or losing data due to irregular backups or weak passwords (Crossler, 2010). At the core of PMT, attitudes of individuals are assessed through two cognitive processes which lead to an increased intention to protect oneself against a potential threat: namely, *threat* and *coping appraisal*.

Threat appraisal comprises the perception and assessment of threat *severity* as well as the personal *vulnerability* to a threat. In our security context, perceived severity of a data breach and one's own vulnerability to fall prey to such an event will affect the protection motivation regarding data. As both perceived severity and vulnerability are positively correlated with the response behavior to protect one's data, which in our case will be through strong passwords, we hypothesize:

H1a. *Perceived vulnerability will have a positive effect on an end-user's intention to protect (work and private) data.*

H1b. *Perceived severity will have a positive effect on an end-user's intention to protect (work and private) data.*

Once the threat is assessed, e.g., the potential severity of data loss or theft and one's susceptibility or likeliness to experience such an incident, individuals will evaluate a potential behavioral response to the threat during the so-called *coping appraisal*.

Coping appraisal includes the concepts *response efficacy* and the associated *response costs* of the planned coping response necessary to protect oneself from the specific threat, as well as one's perceived *self-efficacy* in performing the response. If self-efficacy and response efficacy outweigh response costs, an individual yields a positive coping appraisal, i.e., individuals will install anti-virus software despite the associated costs in terms of purchase price or time to install because they feel capable of performing the installation and also deem the software to be effective in averting viruses and malware (Anderson & Agarwal, 2010; Crossler, 2010). More precisely, response efficacy in PMT refers to the belief that a certain response performed by the individual actually leads to a reduction or elimination of the considered threat.

Regarding IS security, end-users might wonder if strong passwords actually increase the security of their own or their company's data. If this specific response is considered effective in actually decreasing the threat (such as potential misuse of data caused by unauthorized access) an individual will be more inclined towards actually using strong passwords. However, this response also entails the cognitive effort of remembering several complex passwords. The concept of response costs thus assesses all efforts and expenditures associated with the coping behavior which will have a negative impact on the intention of actually performing the response in question. We thus hypothesize:

H1c. *Response efficacy will have a positive effect on an end-user's intention to protect (work and private) data.*

H1d. *Response costs will have a negative effect on an end-user's intention to protect (work and private) data.*

The core nomology of PMT additionally includes the concept of self-efficacy which has also been applied in various other theories to assess IS security behavior, often as part of the construct *perceived behavioral control* (PBC) (Ajzen, 1991, 2002; Boss et al., 2015). On the one hand, self-efficacy relates to the confidence of individuals in their own skill, knowledge and

ability to perform the response. On the other hand, *controllability*, as the second aspect of PBC, describes how much of the performance is actually up to the individual (Ajzen, 2002; Bandura, 1997). One example would be that employees might be hindered to implement a security measure due to missing administrator rights on their work computers. Similar to other PMT-based studies which extended their research model with elements of the models originating from *theory of planned behavior*, we also integrate the complete concept of PBC into our model as it could serve as a differentiator between the work and private context (Anderson & Agarwal, 2010; Workman et al., 2008).

In an IS security context, end-users who are confident in their ability to perform an appropriate security measure like backing up data at home or at their workplace will be more inclined to progress with that chosen coping mechanism. However, controllability might differ across contexts, because employees might not express the same extent of assumed controllability to their action if they cannot implement a security measure due to missing administrator rights, even if they had the skill and knowledge in doing so. As a result, they might shift the responsibility to their IT department or employer. Nevertheless, if employees just like private end-user ascribe responsibility to themselves, i.e., perceive higher degrees of controllability regarding the coping mechanism, they will be more proactive in taking appropriate security measures (Workman et al., 2008). Hence, we expect that:

> ***H1e.*** *Self-efficacy will have a positive effect on an end-user's intention to protect (work and private) data.*
>
> ***H1f.*** *Controllability will have a positive effect on an end-user's intention to protect (work and private) data.*

5.2.2 Psychological Ownership

The following examples help introduce the concept of PO: 1) Alice and Bob, both three year old toddlers, erupt in a fight over a doll in a physician's practice: both children claim the doll belongs to them and attempt to protect it from the other claimant by shouting 'It is MINE!' – Although, technically, the doll is legally owned by the physician. 2) Alice's mother is a project manager. She lovingly calls one of her recent projects her 'baby' and takes many project-related tasks home to continue working after hours instead of delegating tasks because she feels a high sense of commitment and ownership towards this particular project. These scenarios depict how individuals behave when they feel that they possess an ownership stake in a physical or intangible object – a phenomenon called psychological ownership.

PO stems from psychology and describes the sense of ownership of a target like the aforementioned doll or project, but can also be felt towards a concept, other person, or an entire organization or community. The target is seen as an extension of the self (Webb & Sheeran, 2006), i.e., the owners regard the target as an expression of themselves or feel a strong sense of belongingness towards the target – as evidenced for example by football supporters who feel strong ownership towards their football club (Dittmar, 1992; Pierce et al., 2001). Although related, PO is distinct from *legal ownership* which is recognized by society and protected by legislation – whereas PO is a "condition of which one is aware through intellectual perception […] coupled with an emotional or affective sensation" (Pierce et al., 2003, p. 86).

The roots of PO or the reason why this cognitive-affective state exists is best explained by an innate need of having a place or *belongingness* to the target (Duncan, 1981), a sense of symbolic expression though the target or *self-identity* (Dittmar, 1992), and the desire to experience *causal efficacy* through control and accountability over the target (Furby, 1978; Pierce et al., 2001). Due to the versatility of the PO concept, it has found extensive application especially in management and organizational research. More recently, studies in an IS context, have demonstrated the impact of psychological ownership on system usage and appreciation of IT or virtual products (Klesel et al., 2016; Lee & Chen, 2011), willingness to disclose data (Cichy et al., 2014), or intentions to perform security-related behavior (Anderson & Agarwal, 2010; Menard et al., 2018). The latter two studies examine the role of PO as antecedent of the threat and coping appraisal or its direct effect on behavioral intention. The resulting effects on PO have been analyzed and categorized into positive outcomes – such as citizenship, personal sacrifice and assumption of risk, or experienced responsibility and stewardship – and negative effects like territoriality and other defiant behavior, or personal maladies like stress or frustration if the target is subject to any form of alteration (Pierce et al., 2003; Vandewalle et al., 1995).

Thus, threats to the target can be regarded as threats to oneself because the target represents an extension of one's self-concept or identity. In our context, higher levels of PO will lead to heightened perceptions of severity and vulnerability when faced with the prospect of losing one's data. This will more likely occur in the context of private data as opposed to data in a work context. Hence, we assume that risk appraisal will be influenced through psychological ownership as follows:

> ***H2a.*** *PO of (work and private) data will <u>increase</u> perceptions of threat vulnerability. This effect will be more pronounced in a private context.*

H2b. *PO of (work and private) data will increase perceptions of threat severity. This effect will be more pronounced in a private context.*

Intimate knowledge or a deep understanding and familiarity of an object will lead to higher degrees of association with the object (Rudmin & Berry, 1987). This is evidenced by individuals' statements of preferring own targets to comparable others, simply because one knows them better, e.g., the favorite spot in the canteen. Acquiring knowledge about a target is also linked to investment of the self into the target which represents the third route to PO. Investing time, effort, or energy into the creation or development of a target, e.g., in a mentor-mentee relationship or into Do-it-yourself-projects, facilitates feelings of PO by seeing one's own reflection in the target (Pierce et al., 2003). In organizational studies, employees who feel PO toward their company are shown to express higher levels of organizational commitment, organizational-based self-esteem, and job performance (e.g., Avey et al., 2009; Van Dyne & Pierce, 2004; Vandewalle et al., 1995). Subsequently, Pierce and colleagues argue that pronounced feelings of PO will influence the degree of its effects – both positive and negative (Van Dyne & Pierce, 2004). In line with Menard and colleagues, we also expect that PO will exert influence on the coping appraisal considering the use of diverse and strong passwords in both the private and work context (Menard et al., 2018) and thus hypothesize:

H2c. *PO of (work and private) data will increase perceptions of response efficacy. This effect will be more pronounced in a private context.*

H2d. *PO of (work and private) data will decrease perceptions of response costs. This effect will be more pronounced in a private context.*

Apart from intimate knowledge of the target, and investment of the self, Pierce and colleagues also argue that perceived control is closely tied to feelings of PO (Pierce et al., 2001). Numerous studies prove that control is a core feature of ownership as objects that are habitually used or can even be manipulated by an individual become more assimilated into the user's self-concept (Furby, 1978). According to Avey et al., individuals will be "feeling more efficacious about working with the target, feeling more accountable for what happens with respect to the target" (Avey et al., 2009, p. 24) when they feel psychologically tied to the target. In our context, PO regarding their data will thus facilitate feelings of responsibility and as a result lead to heightened levels of willingness and confidence in their ability to carry out a protective response against the IS security threat (Dipboye, 1977).

H2e. *PO of (work and private) data will increase perceptions of self-efficacy. This effect will be more pronounced in a private context.*

H2f. *PO of (work and private) data will increase perceptions of controllability. This effect will be more pronounced in a private context*

5.3 Research Model and Method

Our research model draws primarily on the approach of Menard and colleagues (2018) which examines how psychological ownership affects the protection motivation based on PMT. We further extend the model with the additional construct of controllability in order to include and examine another important but yet often overlooked aspect of perceived behavioral control. In both contexts, we examine how the behavioral intention to use strong passwords in order to protect data is influenced by both the classic determinants of PMT and how these are in turn influenced by PO in our two contexts

5.3.1 Data Collection Procedure

In order to investigate our research questions, we conducted two consecutive online surveys using the same respondent panel (cohort). We selected currently employed individuals from Germany who use electronic devices to access software applications or websites and are interacting with company data in their professional environment on an everyday basis. In both questionnaires, variables of our research model were surveyed. Whereas the survey conducted first focused on the participant's professional work context, we repeated testing our research model in a second wave by focusing on the private use of IT devices. As threat scenario we chose the misuse of data caused by insecure passwords. Consequently, the coping strategy depicted the usage of strong passwords which are distinct between different user accounts.

Both questionnaires were distributed online in August 2018 in two waves with the help of a market research institute: respondents first answered a survey assessing their password behavior at their respective workplace. Seven days upon completion, the same cohort was invited to participate in a second survey assessing their password behavior within their private context. This timespan was chosen in order to avoid manipulating risk appraisal and coping appraisal between both conditions through unforeseen incidents or factors (work vs. private context) and is comparable to other IS studies with a longitudinal design within (Kehr & Kowatsch, 2015; Milne et al., 2002). Both surveys commenced with a welcome page which ensured the participants' anonymity and that there are no "wrong" answers in order to counteract common method biases (Podsakoff et al., 2003).

Only those participants who completed both survey questionnaires were included in the data analyses. Accordingly, despite 297 completed questionnaires in the first wave, only 217 data sets were further analyzed after the second wave. Since eight participants failed our attention check during the second wave, their answers were deemed unreliable. The final sample size was thus 209. The effective response rate – after eliminating unreliable responses and attention checks – amounted to 70.37 percent, an acceptable rate for questionnaires considering security-related behavior (Crossler, 2010; Sonnenschein et al., 2017).

The sample was evenly distributed in terms of gender (51.2 % female; 48.8 % male) and age (mean = 44.9; min = 19; max = 65) through quotas mirroring the percentage of the overall population in Germany thus providing an adequate snapshot of reality of German employees. We report a more detailed sample statistic in the online appendix (Table A1)

5.3.2 Operationalization of Research Variables and Instruments

All measurements to operationalize our research variables are based on previously validated operationalization and have been adapted to the context of our study as we report in the online appendix (Table A2). The items for all threat related PMT constructs (vulnerability [VULN], severity [SEV]) were adopted from Johnston and Warkentin (2010). Items for response efficacy [RE] have been extracted from Witte (1996) whereas response costs [RC] as well as self-efficacy [SE] were adapted from Milne at al. (2002). Controllability [CON] was measured using the scale from Kraft and colleagues (2005). Our dependent variable behavioral intention [INT] has been operationalized using items from Herath and Rao (2009) whereas psychological ownership [PO] has been adopted from van Dyne and Pierce (2004).

5.4 Data Analysis and Results

Our data set contains 209 responses for each context based on the same respondent cohort. Therefore, we distinguish between two contexts: the work versus the private context. In the following, the hypothesized relationships between variables are analyzed relying on the PLS algorithm as implemented in SmartPLS in order to simultaneously validate the measurement model and the conceptual path model (Bagozzi & Yi, 1989).

Measurement Model Testing. We begin by assessing convergent validity of all our variables for each condition (work and private). Internal consistency can be assumed for constructs if Cronbach's alpha (Cr α) as well as composite reliability (CR) are at least 0.7 (Bagozzi & Yi, 2012). To establish convergent validity, the average variance extracted (AVE) should exceed

0.5 (Hair et al., 2013). In addition, item loadings are assessed against a threshold of 0.65 or higher (Falk & Miller, 1992). We find minimum loadings of 0.707 / 0.840 in the work and private context respectively. Therefore, we conclude that convergent validity is ensured.

	Work Context										
	Cr α	**CR**	**AVE**	CON	INT	PO	RE	RC	SE	SEV	VULN
CON	.915	.937	.790	**.889**							
INT	.948	.967	.906	.383	**.952**						
PO	.906	.941	.843	.167	.095	**.918**					
RC	.940	.957	.848	.252	.403	-.054	**.896**				
RE	.879	.924	.803	-.248	-.399	-.047	-.223	**.921**			
SE	.854	.912	.775	.236	.469	.015	.387	-.662	**.880**		
SEV	.927	.948	.821	.273	.355	.060	.361	-.126	.315	**.906**	
VULN	.794	.859	.606	.004	.001	.192	-.061	.237	-.116	.102	**.778**
	Private Context										
	Cr α	**CR**	**AVE**	CON	INT	PO	RE	RC	SE	SEV	VULN
CON	.937	.954	.840	**.916**							
INT	.930	.955	.876	.366	**.936**						
PO	.888	.931	.818	.437	.297	**.904**					
RC	.949	.963	.867	.582	.364	.446	**.898**				
RE	.881	.926	.807	-.354	-.446	-.199	-.070	**.931**			
SE	.881	.927	.810	.399	.514	.333	.189	-.746	**.900**		
SEV	.929	.950	.825	.252	.260	.306	.364	-.080	.137	**.909**	
VULN	.898	.928	.762	-.235	-.102	-.067	-.171	.356	-.209	.095	**.873**

Table 8. Measurement Model Validation

For acceptable discriminant validity, we rely on the criteria suggested by Fornell and Larcker (1981). Accordingly, the square-root of AVE (**bold** numbers in Table 1) needs to be greater than the correlations to all other constructs. Since this holds true for all constructs within both conditions, we assume our measurement model to be accurate as further evidenced by cross loadings reported in the online appendix (Table A3).

Structural Model Testing. Continuing with the validated measurement model, we assess the overall model fit of our conceptual models. The standardized root mean square residual (SRMR) is 0.066 resp. 0.046 (work resp. private) which is well below the cutoff-point of 0.08 recommended by Hu and Bentler (1998), indicating a good model fit. The amount of variance explained within our dependent variables (R2) are presented in Figure 1. We use a bootstrapping procedure with 5,000 subsamples to test for statistical significance of path coefficient estimates which results are also reported.

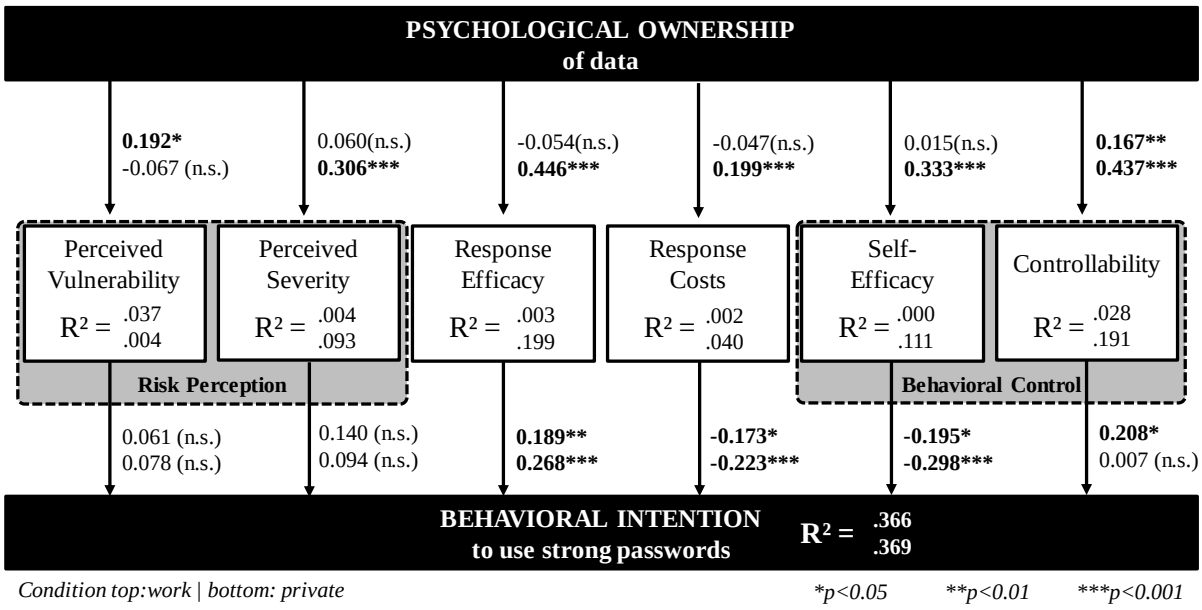

Figure 8. Results of the PLS Model Estimation

Work context. In the work context, all dependent variables based on PMT (H1 c, d, e, f) except for risk perception are supported. Furthermore, psychological ownership of data shows only significant influences on the variables perceived vulnerability (H2a) and controllability (H2f).

Private context. The results show that risk perception has no significant influence on behavioral intention to use strong passwords in the private context. Nevertheless, response efficacy, response costs and self-efficacy significantly influence behavioral intention to use strong passwords and thus support H1c, d, e. The expected effect of controllability on behavioral intention is not supported. However, perceived ownership of data has a strong influence an all PMT related constructs except for perceived vulnerability as well as controllability (H2b, c, d, e, f supported).

Multi Group Analysis. As an extended analysis of the differences between the two contexts, we conducted a multi group analysis. Due to space limitations we report hypotheses which ultimately show significant differences in their path-coefficients only in our online appendix (Table A4). Hereby, the context shows a mediating effect on H1f and H2a as the effects are stronger in the work context compared to the private context. The context furthermore mediates all other relations from psychological ownership. Hence, the effect of psychological ownership is stronger in the private context compared to the work context for H2b, c, d, e, f.

5.5 Discussion and Contribution

With this study, we contribute to a better understanding of PMT according to the situational context and via an extension through PO. By using a longitudinal repeated measures design, we are able to demonstrate varying mechanisms leading to the intention to protect either private or work data through strong passwords. Specifically, our results demonstrate that risk appraisal through perceived severity and vulnerability does not significantly affect the intention to use a security measures such as strong passwords which is in line with some recent findings of other researchers (e.g., Boss et al., 2015; Menard et al., 2018).

Furthermore, we find significant differences regarding the effect of controllability across contexts: whereas a significant effect of controllability on the intention to use strong passwords indicates that employees feel accountable for their choice, this effect could not be shown among private end-users. This might indicate that they do not even perceive an opportunity to shift control, and thus accountability, to some third party such as the employer. Therefore, we find evidence that individuals in the private context are aware of their sole accountability when responding to security threats. Otherwise, we found the influence of coping appraisal to be generally stronger in a private context.

Similarly, but opposed to the study of Menard and colleagues (2018), we could demonstrate lesser and mostly insignificant effects of PO on PMT antecedents in a work context. PO effects are – with the exception of controllability – only significant in a private context apart from the hypothesized influence on perceived vulnerability – which, in turn, is only evident in a work context. Additionally, a post-hoc performed paired t-test ($t(208) = -20.36$; $p < 0.001$) of PO according to the condition work ($M = 3.07$; $SD = 2.77$) or private context ($M = 5.89$; $SD = 1.34$) showed significant differences. Accordingly, we can subsume that PO is more pronounced considering the protection of private data and, as individuals tend to evaluate a target more favorably when they own it, feelings of accountability, responsibility, and investment of the self in the target are stronger (e.g., Avey et al., 2009; Pierce et al., 2003; Van Dyne & Pierce, 2004). This leads to several potential implications for both theory and practice.

Theoretical Contributions. From a research point of view, our approach is the first to our knowledge that is based on a longitudinal repeated measures design which enables the comparison of PMT's explanatory power in a work and private context based on the same safeguarding behavior, i.e., the use of strong passwords. Our study contributes to an improved understanding of the relationships within the theory and shows varying support of the general concepts of risk and coping appraisal. Risk perception in isolation does not promote safeguarding measures in

any context, whereas the inclusion of controllability could contribute to more thorough understanding of employee intention regarding the use of strong passwords. Additionally, our findings contribute to the still scarce literature on psychological ownership in IS security. IS research and studies on and information security in particular, have incorporated PO very rarely and diversely in terms of context and the mode of influence which calls for replication studies as called for by Menard et al. (2018) or Anderson and Agarwal (2010). In this regard, we could demonstrate that PO significantly influences several PMT antecedents only in a private context and barely affects the protection motivation among employees. Furthermore, a direct influence on intention was not found in both contexts as opposed to the aforementioned studies which could be related to the differences in targets as one's own device might elicit more pronounced feelings of PO compared to intangible data or the operationalization of PO through scenario manipulation (Davison & Martinsons, 2016).

Practical Implications. As such, our study informs IS scholars but also practitioners about how a sense of ownership can regulate protection motivation and thus lead to the actual use of safeguarding mechanisms like strong passwords. Practitioners in particular should stimulate feelings of PO regarding company data in order to increase protection motivation. PO can herein be increased and stimulated by tapping into its antecedents, e.g., through more intimate knowledge of the target, in our case data, and also more time and effort invested into understanding how data can be protected, employees will develop a feeling of freedom of choice and more accountability (Klesel et al., 2016).

5.6 Conclusion, Limitations, and Future Research

Despite taking all necessary measures to ensure qualitative results, our study is not without limitations. In this regard, a typical limitation of behavioral IS theories is the measurement of intention rather than actual behavior. Although intention is widely regarded to be a very robust predictor of actual behavior (Ajzen, 1991; Fishbein & Ajzen, 1975), future research could build onto our findings with an experimental design that observes the influence of PO on actual behavior. Similarly, previous research has identified several other influencing factors like culture or personal characteristics which had to be omitted due to duration constrains but could enhance our understanding about the modes of action of PO in an organizational and individual security context. Especially, since culture has been shown to have an effect of the level of PO expressed, our results could be culturally constrained to Western, more individualistic, cultures (Menard et al., 2018). From a methodological point of view, the rather short timeframe of our two sur-

veys might add to the general finding that humans strive for a consistent manner of self-representation which might result in memory effects or so-called experimenter demand effects (Kehr & Kowatsch, 2015; Podsakoff et al., 2003). However, an extension of the time frame might be affected by unidentifiable external influences due to unforeseen incidents or other biases that arise during the survey period.

An avenue for future research could be the analysis of PO antecedents through an action research design measuring whether increased feelings of PO also lead to improved actual security behavior in both a work and a private context. Our study thus serves as an important stepping stone which first compared the behavior of individuals in these contexts in a repeated measures design revealing varying degrees of effect sizes in well-established PMT and newly hypothesized PO relationships. Furthermore, future research could develop a new operationalization of PO for the IS context, as current measures are often based on physical, tangible targets. A different approach could be the use of an Implicit Association Test which can detect underlying attitudes of users or consumers particularly when subjects are unaware or unwilling to identify sources of influence – like PO in our context (e.g., Brunel et al., 2004).

6 Paper C: A Holistic View on Organizational IT Security

Title

A Holistic View on Organizational IT Security: The Influence of Contextual Aspects During IT Security Decisions

Authors

- Margareta Heidt, Technische Universität Darmstadt, Germany
- Jin P. Gerlach, Technische Universität Darmstadt, Germany
- Peter Buxmann, Technische Universität Darmstadt, Germany

Publication Outlet

Hawaii International Conference on System Sciences (HICSS), Wailea, USA. VHB-Ranking: **C**.

Abstract

Decisions regarding organizational IT security are often approximated by models drawing on normative statistical decision theories even though several IS researchers and studies in cognate disciplines have argued for the importance of contextual aspects. Based on findings in organizational and behavioral science and 25 expert interviews, this paper proposes a framework, postulating that IT security (investment) decisions are largely influenced by such contextual aspects: organizational, environmental, economic, and not least of all by cognitive and behavioral aspects of decision-makers.

Subsequently, we review organizational IT security literature building on Straub and Welke's Security Risk Planning Model and the previously postulated conceptual framework. This critical literature review highlights the scarcity of studies analyzing IT security decision-making from a behavioral, environmental, and organizational perspective and thus argues for the importance and future consideration of contextual aspects regarding IT security decisions.

Keywords

Decision, Investment, IT Security, Risk Planning Model, SME

6.1 Introduction

"Risk analysis techniques (financial costs of event multiplied by probability of event equals exposure) are not appropriate where business survival is at issue" (Newton, 1985 based on Baskerville (1991)) – since the early phase of the Information Systems (IS) discipline, researchers and practitioners like the above-quoted Newton (1985) have pointed out the complexity of risk identification, assessment and the subsequent decision-making regarding information systems security and the thus limited applicability of purely statistical and normative approaches.

However, the predominant approach regarding organizational decisions about IT security remains heavily influenced by purely quantitative models and theories that mainly highlight economic aspects of investment decisions (e.g., Bodin et al., 2005; Cavusoglu et al., 2004; Cavusoglu et al., 2015) but do not consider organizational, environmental, and behavioral aspects (i.e., context). Especially, studies focusing on risk analysis as an aspect of the decision-making process continue to draw on statistical decision theory despite the de facto deviation from this normative approach in practice (e.g., Baskerville, 1991). Recently however, commonly employed cost-benefit analyses (e.g., Khansa & Liginlal, 2009) or the consideration of institutional factors (e.g., Angst et al., 2017; Cavusoglu et al., 2015) increasingly acknowledge the presence and influence of economic, organizational or environmental aspects during the IT security decision process.

Meanwhile, decade-old findings from behavioral economics and decision sciences have not been adopted sufficiently by IS researchers as pointed out by former MIS Quarterly Editor-in-Chief Paulo Goes (2013) or Crossler and colleagues (2013). Both articles reinforce "that the context matters in how the cognitive effects [as stated by behavioral economists] influence the choices" (Goes, 2013, p. vii) and advocate the necessity to consider contextual factors in security and privacy studies given the highly complex nature of current IS environments.

Against this backdrop, this paper proposes a conceptual framework that builds on insights from organizational IT security research before employing a qualitative approach to identify which contextual aspects affect decision-makers in predominantly small and medium-sized enterprises (SME) regarding the decision-making process in organizational IT security through 25 expert interviews. Small and medium-sized enterprises have been particularly overlooked by IS security literature which continues to focus on large enterprises within specific industries, i.e., healthcare and finance (e.g., Angst et al., 2017; Huang et al., 2014) although SME account for more than 95% of enterprises worldwide (OECD, 1997). Decision-makers in SME however

are directly responsible for their businesses' survival which requires them to take various internal and external factors into account and heightens the influence of individual characteristics when deciding upon investing in IT measures in general, and IT security in particular (e.g., Dholakia & Kshetri, 2004; Thong & Yap, 1995).

Findings of the interview study are derived through a content analysis and provide insight both into the influence of contextual aspects on IT security decisions and into specific nuances of the investment decision such as the provider selection or the area of investment. Drawing on these findings, an in-depth analysis of the extant literature in organizational IT security research depicts which aspects are considered during the IT security decision process and which investment nuances are primarily investigated. In this regard we provide a holistic overview of the current state of research and unveil extant gaps that future research could close and thereby enhance the body of knowledge regarding the influence of contextual factors in organizational IT security decisions.

The remainder of this article is structured as follows: the subsequent section provides the theoretical background which is distilled into a conceptual framework. Subsequently, this framework is used to analyze the content of both expert interviews and extant literature through a semi-directed content analysis. Thereupon, the findings of the qualitative and the literature analysis are presented and synthesized during the discussion before limitations and prospects for future research conclude this paper.

6.2 Theoretical and Conceptual Background

6.2.1 Phases of IT security decision processes

Our initial theoretical lens employed during the analysis of our qualitative study and the subsequent literature review regarding organizational IT security risk is based upon Straub and Welke's (1998) Security Risk Planning Model and Goodhue and Straub's (1991) Model for Managerial Perceptions of Security Risk. Whereas the first model consists of 5 phases, namely (1) recognition of security problems, (2) analysis, (3) alternative generation, (4) decisions, and (5) implementation, the latter argues that the organizational and the IS environment along with individual characteristics strongly influence manager perceptions and thus managerial concern about systems risk.

Both models have been extensively referred to in their pure or modified form in various IT security studies (e.g., Dhillon & Backhouse, 2001). The risk planning model in particular can be considered as the foundation of established process models (e.g., ISO, 2018) and among the

first to build on Goodhue and Straub (1991) by taking socio-organizational factors into account. A focus on the role of decision-makers and managers highlights the influence of their perception on IT security risks and effective controls on organizational IT systems. Due to its high-level conceptual management approach and its recognition of socio-organizational factors such as the IS environment and managerial characteristics, their model provides the core of our conceptual framework. This framework helps to later on identify and contextualize aspects that influence decision-making processes regarding IT security investments.

6.2.2 Organizational decision-making

Decision-making processes in general are usually categorized through the distinction between a normative or descriptive approach (Simon, 1979). Whereas a normative approach focuses on how decisions should be made by employing mathematical models and assuming rational stakeholders, descriptive decision theories attempt to depict how decisions are actually made. In his seminal work on decision-making in businesses, Herbert Simon states that "if human decision-makers are as rational as their limited computational capabilities and their incomplete information permit them to be, then there will be a close relation between normative and descriptive decision theory" (Simon, 1979, p. 499) before arguing for the existence of bounded rationality and the influence of external factors. Thus, the close relation between both theory types is attenuated and the influence of external factors such as legal and social structures promoted. In this regard, IS studies which employ an Institutional Theory approach, have investigated and demonstrated the influence of environmental aspects such as conformity with external norms and social influence on investment decisions (Angst et al., 2017; Salge et al., 2015).

Against this backdrop, a plethora of studies in business investment decisions either follow classic economic approaches such as cost-benefit analyses or value estimations or build on Contingency Theory or a Resource-Based View which acknowledge the distinct influence of external factors such as available resources or organizational structures (Dor & Elovici, 2016; Vroom & Yetton, 1973; Weishäupl et al., 2018).

Based on these findings and influenced by Dor and Elovici's (2016) categories, we aggregate influencing factors into behavioral/cognitive aspects, organizational aspects, environmental aspects, and economic aspects and presuppose their influence on the IT security decisions process introduced by Straub und Welke (1998) as illustrated in the following Figure 1.

In addition, we make a further distinction within the decision phase and propose four nuances as the decision can either be fundamental, i.e., (1) the initial adoption decision whether to invest

at all (Y/N), or directed at the specifications of the intended IT security investment, i.e., (2) where/into what to invest (area or content of investment like recovery or prevention measures on an abstract level; one- or two-factor authentication on a more detailed level), (3) from whom or where to source (self-developed or selection of provider), and (4) how much to invest (level or extent of the investment). These nuances are also depicted in Figure 9.

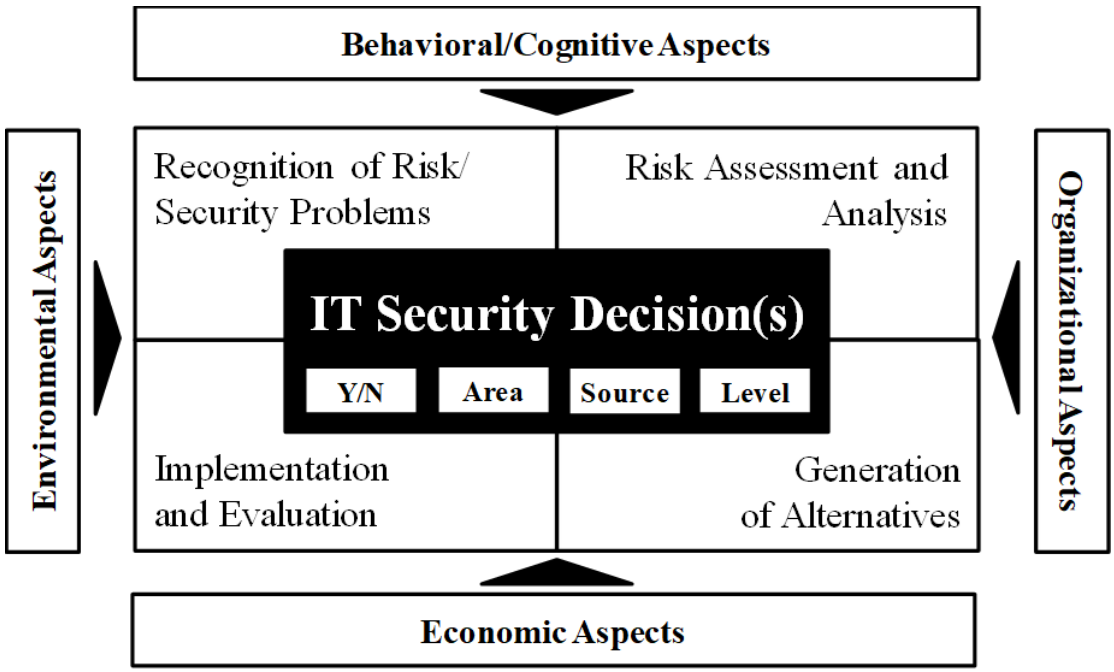

Figure 9. Conceptual Framework of Literature Analysis

6.3 Research Methodology

The conceptual framework is first applied during the analysis of an interview study and the subsequent literature review. Therefore, a robust and versatile method like content analysis can serve both as a tool to analyze qualitative data derived through interviews and in order to review relevant literature thoroughly and comprehensibly (e.g., Hsieh & Shannon, 2005; Mayring, 2014). While this paper predominantly employs a directed content analysis approach as we build on prior research about decision-influencing factors to validate our conceptual framework, we also draw on inductive aspects of conventional content analysis to allow for new insights to emerge from the data (Mayring, 2014).

6.3.1 Research design, sample, and coding process

Drawing on guiding principles for qualitative IS studies (Sarker et al., 2013), we collected our data within a European country through semi-structured interviews with a total of 26 participants from 25 organizations in six industries (namely manufacturing; construction; wholesale and retail; information and communication; professional, scientific and technical activities; administrative and support service; education). These participants were either managing directors (14), IT executives (8), business developers (2), or consultants (2). Whereas 19 experts are employed in pure user companies, 5 experts work in IT provider companies and 2 experts in hybrid companies that offer IT services in addition to their traditional (non-IT) product portfolio. Disregarding one company with roughly 660 employees worldwide but less than 250 in the sample country, all other companies can be unconditionally classified as SME with 28 % medium-sized (50-250 employees), 52% small (10-49 employees), and 16% very small enterprises (1-9 employees). The data collection took place between November 2017 and March 2018 and resulted in over 30 hours of recorded interviews, which were transcribed after mutual agreement and analyzed with the software analysis tool NVivo 12 Plus as demonstrated in Figure 10.

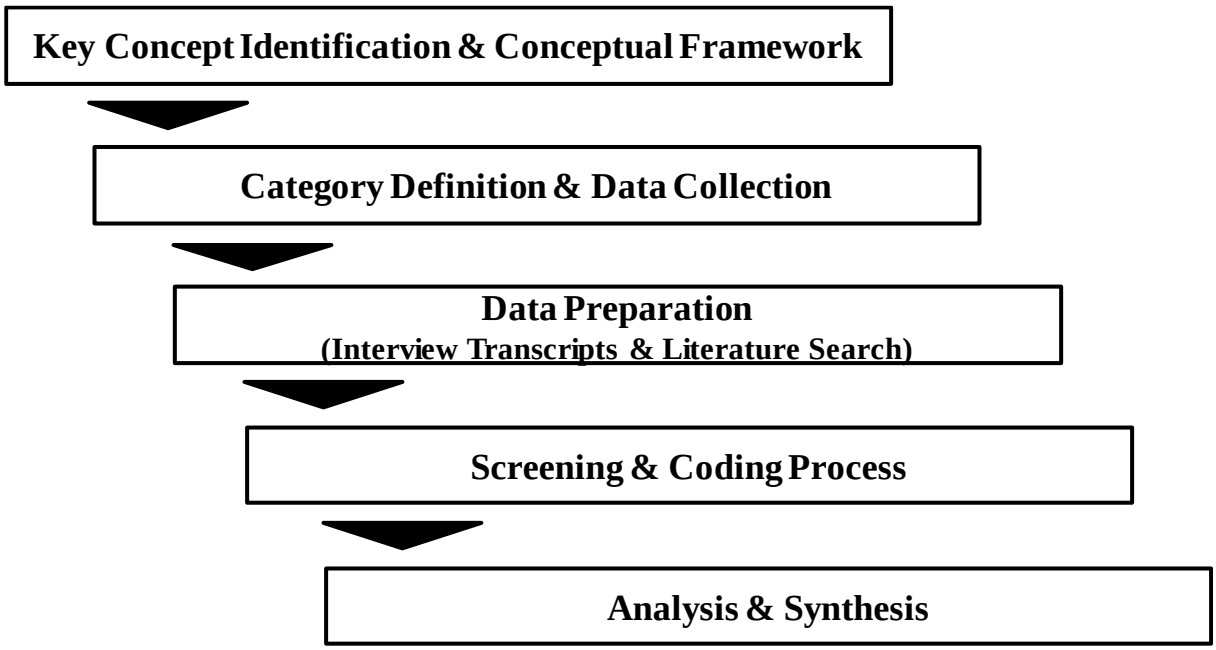

Figure 10. Content Analysis Process (based on Hsieh & Shannon, 2005)

Based on the initial conceptual framework, the transcribed interviews were screened and coded if the description matched the terminology of categories (Dor & Elovici, 2016). Following Mayring's steps of deductive category assignment after the initial screen, subcategories were identified, labeled, and iteratively revised in several coding steps (Mayring, 2014, p. 96). The

final codes were analyzed through coding comparisons and crosstab queries within NVivo. In order to demonstrate rigor and trustworthiness, our coding process followed a clear research agenda, was critically discussed and assessed with several IS researchers, and the selected interviews stemmed from diverse backgrounds including triangulation by including both a user and a provider perspective. Additionally, direct quotes of the subjects contribute to further transparency and accountability.

6.3.2 Findings

In accordance with our proposed framework and focusing on the decision phase, we found evidence that contextual aspects are highly relevant during the decision-making process regarding organizational IT security investments. Especially, behavioral, organizational, and environmental aspects were strongly supported whereas economic aspects could mostly be condensed into cost-benefit analyses and were predominantly mentioned by experts in larger companies.

Environmental aspects were mentioned most frequently, in terms of information sharing activities (through mostly informal networks and partnerships), micro-environment (i.e., customers, suppliers, industry characteristics, and market/competition) and macro-environment (legislation/regulation, global pressure). Especially, legal pressure or certain regulations like the EU General Data Protection Regulation (GDPR) have a profound effect on SME's investment decisions in IT security: they influence the very basic decision whether to invest or not, in what area to invest as well as the extent or level of investment. Due to length restrictions, Table 1 exemplary depicts this category, its concepts and the verbatim quotes taken from the transcribed interviews

We additionally investigated the overall mentions of all aspects via crosstab queries in order to report the relative share of all four categories for descriptive insights (Mayring, 2014). Whereas environmental aspects were most often mentioned (33.74%), behavioral and cognitive aspects followed at 26.67% and organizational aspects at 25.42%. Economic aspects were less frequently mentioned at 15.34%.

All contextual aspects were further fragmented into the identified subcategories, e.g., environmental aspects were subdivided into micro- and macro-environmental elements such as the influence of the industry, customers or state-level legislation and regulations affecting the organization on an abstract level. Whereas a further subcategory comprising elements of social influence and information sharing relates to the environment of the individual. These subcategories are enriched by verbatim quotes and the identified effect on nuances of the investment

decision. By means of example, we could identify that requirements or auditing activities posed by customers or regulations exhibit a strong effect on the initial adoption decision whether to invest at all into IT security and the particular area of investment, e.g., recovery measures such as data backups and archives. Social influence via predominantly non-formal information sharing also directs decision-makers towards the area of investment as well as the sourcing option, i.e., provider selection.

	Manifestation		Effect on Investment Nuance			
	Subcategories and Verbatim Quotes	**%**	**Y/N**	**Area**	**Source**	**Level**
Environmental Aspects [29.58%]	Micro Environment	**44.15%**	**+**	**+**	**o**	**o**
	"Because customers today actually require […] that you are ISO certified, because they say that they also have to adhere to these terms […]" Firm I, CIO (User)					
	Marco Environment	**31.29%**	**+**	**+**	**o**	**+**
	"It (IT security investment) appears on the agenda with the GDPR and because it is a required course, it gets the necessary priority", Firm J, MD (User)					
	Information Sharing/Social Influence	**23.93%**	**o**	**+**	**+**	**o**
	"Through our association […] or simply via wisdom-of-the-crowds where we just ask around for experiences like 'that's what we need, what would you say?'. Or we ask friendly competitors for insights into what the use and why.", Firm M, MD (User)					
+ = stated positive effect; **o** = no clearly stated effect; **-** stated negative effect						

Table 9. Exemplary Qualitative Study Findings

Behavioral or cognitive aspects also appear to have a profound effect on investment decisions: individual managerial characteristics such as the awareness level, risk attitude or a traditional mindset along with certain biases and the strong reliance on "gut feeling" were found to exert influence on all nuances of the investment decision. In addition, experiences with IT security incidents and resulting risk recognition have ripple effects throughout all decision phases and on several investment nuances as evidenced by the following quote:

"Everyone has their own attitude: there are the ones that are saying that security is worth every penny and others are more like 'ugh, we don't need all of that, it'll work out somehow'", Firm N, Business Developer (Provider)

Organizational aspects mostly cover the respective firm's resources, its structure and processes along with "softer" factors such as culture or strategy. Resources like budget, manpower, time or culture and strategy strongly impact the decision whether to invest at all in IT security.

"How difficult will it be to implement it? And also, which and how many resources do we need? […] How much budget will it require? And then it's time to decide or to deliberate. In favor or - not too often – against", Firm M, Managing Director (User)

Additionally, the firm's culture and tradition have a strong effect on the investment source, i.e., the selected provider due to the increased relevance of trust and ingrained sourcing relationship. Meanwhile, structure and processes often define the area of investment, whereas available resources also often determine the extent of IT security investments.

In a similar vein to the aforementioned quote, economic aspects along with value estimations, return on investment (ROI) calculations and general economic tools and methods were surprisingly less influential during the decision phase and were – if at all – only rudimentarily employed during risk analysis (phase 2) or alternatives generation (phase 3). Even after being specifically asked about economic tools, most interviewees either mentioned that they do not see how these methods support IT security decisions or explicitly mentioned that indicators like the ROI are only calculated to please managing directors. All in all, only budgeting (or the lack thereof) and initial cost-benefit analyses (CBA) exerted influence on investment decisions. In this regard, particularly IT executives and interviewees at provider companies expressed the necessity of a more formalized budgeting process which is currently missing in the majority of SME.

"Oh well, of course you can try to somehow calculate the ROI […]. That might be important in large enterprises […] but here arguments are far more important. Here, we have to make sure that the solution fits in financially", Firm Q, CIO (User and Provider)

In summary, especially environmental aspects such as customers, legislations but also social influence and information sharing appear to have a profound effect on IT security investment decisions and their nuances. Due to the central role and the numerous responsibilities most decision-makers and especially managing directors in SME possess, the influence of distinct behavioral and cognitive aspects is likely more intense than in bigger companies whereas the necessity to employ elaborate methods to assess economic aspects other than budget constraints and simple cost-benefit techniques are largely negated. Organizational aspects on the other hand are often taken into account as a decision for a particular IT security measure is regarded as a direct trade-off to other organizational investments into the workforce or processes and products.

Based on these insights, we review the current IS security literature to analyze how the identified contextual aspects are currently accounted for and thus subsequently uncover the most prevalent gaps for future research.

6.4 Literature Analysis

In the following section, we provide an overview of our literature review method and the utilized tools. In order to ensure rigor and replicability, we adhere to clearly defined guidelines through a combination of several approaches prevalent in IS research (e.g., Cooper, 1988; Okoli & Schabram, 2010; vom Brocke et al., 2009; Webster & Watson, 2002). Our literature review is structured following Okoli and Schabram (2010) and visualized in Figure 11:

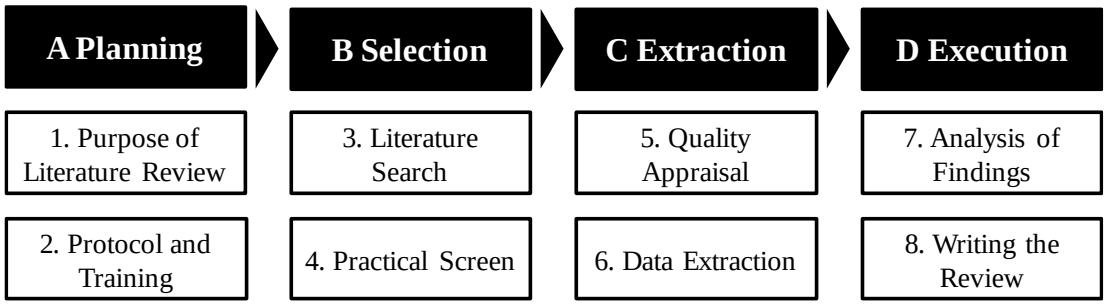

Figure 11. Literature Review Process)based on Okoli and Schabram 2010)

6.4.1 Search and selection strategy

In accordance with Figure 3, we first defined the purpose and review scope before conceptualizing the general topic. The literature search was performed following an explorative search using Business Source Premier and Google Scholar to achieve a better understanding of the topic, synonyms, and the existing research landscape. This resulted in the identification of an appropriate search term as indicated in Table 2. We screened the following databases: AIS Electronic Library (AISeL), Business Source Premier (Ebsco), and Science Direct (SD) along with Web of Science (WoS). Drawing on Cooper (1988), we opted for an exhaustive selective coverage and thus searched by title, abstract, and keywords and arrived at 4295 initial total hits including 140 duplicates. During the selection phase, initial title and abstract screening, which served as practical screen, the analyzed literature was drastically condensed. Thus, only a total of 220 articles were further scrutinized during the extraction phase because they explicitly focused on IT security from an organizational rather than technical or legal perspective. A clustering process ensued along with a quality screen that excluded articles that were published outside of leading IS outlets as defined by Lowry (2004) leading to a total of 87 remaining

articles. Full text-screening was combined with the conceptual framework: all articles which did not or only marginally cover phase 4, i.e., the actual decision phase according to Straub and Welke's (1998) model were excluded along with conference proceedings which were subsequently extended into journal publications resulting in a total of 31 articles (e.g., El-Gayar & Fritz, 2010; Huang et al., 2014). A backward and forward search revealed eight relevant publications which were not identified via the initial search term due to ill-fitting keywords (e.g., Lee & Larsen, 2009). These articles were analyzed following the same approach and criteria.

The rather extreme condensation of the initial total hits can be largely explained with our choice to draw on Cooper (1988). Whereas the search term example aimed at an exhaustive coverage and thus included several keywords that are highly prevalent in numerous studies, the following iterative screening process pursued a selective approach. Selection criteria were mostly determined by the theoretical framework and the resulting focus on the decision process. As a result, publications like Angst and colleagues' (2017) investigation of institutional factors in healthcare security investment which detail the evaluation and implementation of investments rather than the decision process leading towards the investment, were excluded. Similarly, Baskerville's (1991) study on risk analysis covers only the second phase of Straub and Welke's (1998) model and was thus suspended after full text screening. Additionally, literature reviews and meta-studies that primarily systemize IS security literature without identifying further aspects of investment decision (e.g., Dhillon & Backhouse, 2001) were omitted from further analysis.

Detailed exclusion criteria such as a focus on end-users or compliance and employees misconduct along with the exact number of screened articles can be extracted from Table 10.

Search term example	*tak("information security" OR "IT security" OR InfoSec OR InfSec OR cybersecurity OR "data security" OR (securing information assets) OR technology security OR protect* OR "cyber security") AND tak(investment or investing or econom* OR (risk and benefit) OR finance* OR spend* OR judg* OR decisi* OR deciding OR adopti* OR choice OR evaluate* OR choosing OR cost AND NOT (consumption OR marine OR medicine OR agricultur* OR eCommerce OR environmen* OR employment OR energy OR food OR smog OR food OR ecolog* OR protectionis* OR "social media" OR "social network" OR "knowledge management" OR cloud OR "cloud computing" OR ERP OR CRM OR "data warehouse*" OR "data mining" OR eLearning OR "product development" OR RFID OR semantic OR remuneration)*				
	Ebsco	SD	AISel	WoS	Total
Initial Search	**805**	**2066**	**1058**	**366**	**4295**
Articles remaining after Title Screening (initial screen exclusion criteria: publication type (e.g., editorials); discipline (finance, environment, etc.); second screen: no apparent IT (security) focus)					**524**
Articles remaining after Abstract Screening (exclusion criteria: domain (purely technical or legal); context (government, individual enduser behavior), or IT security only tangential)					**220**
Articles remaining after Clustering (exclusion criteria: stock value, cyber-insurance, etc.)					**165**
Articles remaining after Quality Screen (inclusion criteria: leading IS and journals and conferences)					**87**
Articles remaining after Full Text Screening (exclusion criteria: sample (employees, end users); topics (employee misconduct, policy and compliance); no focus on decision-making process)					**31**
Articles after Forward and Backward Search					**39**

Table 10. Structured Literature Review (based on vom Brocke et al. 2009)

6.4.2 Literature analysis

In contrast to existing literature reviews and meta-studies (e.g., Dhillon & Backhouse, 2001; Schatz & Bashroush, 2017) on organizational IT security and investment decisions, our analysis is based on a qualitatively validated framework and includes aspects other than only economic valuation or socio-organizational perspectives. Further, the execution phase of the analysis and synthesis stage was performed through a thorough content analysis based on the theoretical framework adapted from Straub and Welke (1998) combined with the identified and extended contextual factors and investment nuances derived through the qualitative interview study in SME companies. As opposed to previous literature reviews, a distinct SME perspective – which has been largely neglected by organizational IT security research in general – added another analysis layer. Thus, the analysis of the final selection of all 39 articles which can be found in the online appendix also considered whether the respective study focused on an SME context.

Evidently, most studies largely focus on economic aspects of IT security decisions by proposing a value-at-risk or return on (security) investment approach (ROSI) (e.g., Lee et al., 2011; Sawik, 2013; Wang et al., 2008). This is also reflected by the slight surplus of predominantly normative studies (56%) based on mathematical modelling (64% proportionately) (Altinkemer & Wang,

2011; Cavusoglu et al., 2004; Cavusoglu et al., 2008; Dutta & Roy, 2008; Ekenberg et al., 1995; El-Gayar & Fritz, 2010; Fielder et al., 2016; Finne, 1998; Gordon & Loeb, 2006; Grossklags et al., 2008; Guarro, 1987; Gupta et al., 2006; Herath & Herath, 2008; Huang et al., 2014; Khansa & Liginlal, 2009; Kim & Lee, 2007; Kolfal et al., 2013; Lee et al., 2011; Liu et al., 2011; Miller et al., 2016; Nazareth & Choi, 2015; Rees et al., 2011; Ryan & Ryan, 2006; Sawik, 2013). Whereas two studies pursue a purely qualitative approach (Dor & Elovici, 2016; Qian et al., 2012) and six are purely conceptual (Baker et al., 2007; Barnard & Solms, 2000; Baskerville, 1993; Kwok & Longley, 1999; Purser, 2004; Wood, 1988), eleven studies employ a combination of several approaches (Bodin et al., 2005; Cavusoglu et al., 2008; Ekenberg et al., 1995; El-Gayar & Fritz, 2010; Fenz et al., 2011; Fielder et al., 2016; Kim & Lee, 2007; Lee et al., 2011; Miller et al., 2016; Straub & Welke, 1998; Wang et al., 2008) and three are based on panel data (Cavusoglu et al., 2015; Lee & Larsen, 2009; Young & Windsor, 2010).

As already indicated, our search strategy was directed at studies that explicitly focus on the actual (investment) decision, i.e., phase 4 in Straub and Welke's (1998) risk planning model. Several studies focus on a specific investment decision, e.g., investing in a particular authentication system (Altinkemer & Wang, 2011) or an intrusion detection system (Cavusoglu et al., 2004). Other studies propose a generic model and use a specific tool or application as example (Herath & Herath, 2008; Kim & Lee, 2007). The investment nuances that are most often considered in these specific investment studies, but also in publications that pursue a more generic approach, are the specific area or content and the optimal level of investment (Baker et al., 2007; Bodin et al., 2005; Fenz et al., 2011; Herath & Herath, 2008; Huang et al., 2014; Lee et al., 2011; Purser, 2004; Rees et al., 2011; Sawik, 2013). Only a single study is dedicated towards to the decision regarding the source or origin of the investment (Kim & Lee, 2007) and a total of six studies consider the fundamental decision whether to invest at all (Dutta & Roy, 2008; Grossklags et al., 2008; Herath & Herath, 2008; Lee & Larsen, 2009; Qian et al., 2012; Ryan & Ryan, 2006).

The extensive focus on investment nuances such as the specific area of the investment (53%) and the optimal level (49%) is often in line with the intended audience or the specific sample of the respective study. This was determined either by analyzing descriptive statistics in the result section (sample) or the stated practical contributions (audience). More than 53% of studies are directed at decision-makers with a pronounced IT focus such as IT executives and CIOs (e.g., Bodin et al., 2005; Cavusoglu et al., 2015; Sawik, 2013) or take a company level perspective (e.g., Fielder et al., 2016; Huang et al., 2014; Purser, 2004). Executives with a non-IT or

business background like CEOs, managing directors, and business executives were only considered by a third of all studies, whereas provider or employee perspectives could be found in a total of five studies.

The shortage of studies looking at non-IT decision-makers hints at the non-generalizability of their results for the SME context: many SME executives do not possess a particular IT background or extensive knowledge and could thus be best compared to other non-IT decision-makers. Further, only two of the analyzed studies focus explicitly on the SME context (Fielder et al., 2016; Lee & Larsen, 2009) and a handful consider organizational aspects like budget constraints and additional resource restrictions such as a limited workforce which are all highly prevalent in SMEs as pointed out by several SME studies (e.g., Dholakia & Kshetri, 2004; Salavou et al., 2004; Thong & Yap, 1995).

In total, slightly more than half of all analyzed studies consider organizational aspects, most often regarding the available resources in terms of budget or workforce as decision criteria during IT security investments. Even more prevalent and often directly connected to the aforementioned subcategory of organizational aspects are considerations of budgeting activities and especially cost-benefit analyses (61%). However, only a few studies point out specifically that "the selection of security controls should be driven by business needs" (Barnard & Solms, 2000, p. 185) or that "the security budget is set exogenously by management decision" (Dutta & Roy, 2008, p. 370). The latter study is one of the few that highlights the necessity of a holistic view that integrates technology and organizational with behavioral aspects.

Even though we did find evidence in 15 studies of behavioral and cognitive aspects, most of them approach decision-making only from a cognitive point of view, i.e., focusing on analytical or deliberative decision-making processes of decision-makers or their risk attitude. Only six studies account for emotional factors or other behavioral aspects like certain managerial character traits (Dor & Elovici, 2016; A. Dutta & Roy, 2008; El-Gayar & Fritz, 2010; Lee & Larsen, 2009; Straub & Welke, 1998; Wood, 1988). With regard to organizational aspects, decidedly fewer studies consider the influence of the micro- (15%) or macro-environment (20%) of the organization or social influence and information sharing (8%) on the decision process. The most prominent subcategory, macro-environment, solely regards regulations or specific legislations to have an impact on investments. However, with the exception of Purser's study (2004), this influence is considered to affect the area or content of the analysis (e.g., data protection laws promoting backup strategies) rather than stating the connection of legislations on the fundamental decision to invest altogether.

6.5 Discussion

In the following, we will discuss and synthesize our major findings from both the qualitative study and literature analysis.

Similar to Dhillon and Backhouse (2001), our literature analysis demonstrates how current IS security research still heavily relies on normative approaches assuming purely rational decision-makers or the existence of formalized decision processes. Contrary to these assumptions, evidence from organizational research, behavioral economics and more recently neuroscience demonstrates how decision-makers draw on a variety of cognitive shortcuts such as heuristics and biases (e.g., Goes, 2013; Salavou et al., 2004), how decisions are better approximated by behavioral game theory which takes individual characteristics, time perspectives, and trade-offs into account (Camerer, 2003), and how a multitude of factors is usually consulted in organizational IS decision-making (e.g., Salge et al., 2015).

Particularly in an SME context, findings from our qualitative study suggest that decision-makers are heavily influenced by their environment, individual characteristics, and certain characteristics of their organization, in particular resource constraints regarding budget, workforce, but also time and knowledge. These factors in turn restrain the use of economic tools and methods like ROI estimations which prevail in the analyzed studies (e.g., Lee et al., 2011; Sawik, 2013; Wang et al., 2008). Exemplary, many managing directors in a dual role mentioned that they are aware of cost-benefit analyses and ROI or even ROSI estimations but limited time and often inadequate data necessary for such economic calculations are hindering their application in practice.

Surprisingly, the majority of interviewed companies do not perform IT budgeting and investments in IT, or more specifically in IT security, are often viewed as exclusive expense associated with no visible benefit. Decision-making processes thus include cost (rather than benefit) analyses, but the final decisions are often based on gut feeling rather than ‘number-crunching’. Additionally, we found evidence that the often stated long-term orientation of family-owned or small businesses does not seem to influence decision-making even though previous entrepreneurial research suggests that investment activities are directed at wealth preservation for future generation (e.g., Lumpkin & Brigham, 2011; Zellweger, 2007). Furthermore, current research is negligent of the multitude of role-identities, i.e., owner as general manager and head of IT. Role-identities, however, have been shown to impact the evaluation and selection of business opportunities and economic decisions (James, 1999; Mathias & Williams, 2014) and their influence was confirmed through our qualitative approach. Individual or behavioral aspects like

these remain largely disregarded in studies IT security decisions and could not be identified during our literature review.

A further discovery is the importance of environmental aspects on IT security decisions: interviewees very often mentioned how customer requirements and frequent quality audits "forced" them to adopt certain data protection and recovery security measures or to establish security policies and processes. Similarly, state-level interventions in terms of regulations also transpired to be the origin of fundamental IT security decisions and defined the area and level of investment. These factors along with social influence are largely neglected by extant IS security research even though peer influence has been consistently shown to impact organizational decision-making (Aral & Walker, 2011). Especially, the GDPR appeared to have rather large rippling effects as decision-makers in SME feel forced to deal with data protection and security issues in order to avoid possible sanctions. Whereas individual IT security research has, for example, employed General Deterrence Theory to account for such mechanisms (Lebek et al., 2014), current organizational research in this regard has overlooked how regulation affects certain nuances of IT security investment decisions.

Regarding the influence of customers, we could identify first evidence into how IT security investments are increasingly considered as a potential profit center by younger firms in our SME sample. These firms regard IT (security) investment as an economic opportunity or incentive which could increase customer loyalty or acquisition – a point of view that is seldom accounted for by IT security studies (Crossler et al., 2013).

6.6 Conclusion, Limitations, and Future Research

This paper is among the first studies to display the present state of research regarding IT security investments with respect to various contextual aspects that were identified via in-depth interviews with decision-makers in SME. Based on a structured literature review, important research gaps are uncovered which can serve as a first step towards future research endeavors that pursue a holistic view of IT security decision-making.

The contribution of this paper is twofold: first, our qualitative analysis not only confirms the assumption that IS security decision-making processes are affected by various contextual aspects (e.g., Dor & Elovici, 2016; Wood, 1988) but zooms in on the particular context of SME and thus uncovers the most prevalent and significant influencing aspects in this – still rather

neglected – context. Further, we identify that these aspects also vary in their influence on investment nuances which could serve as a first step to uncover the reasons why SMEs still refrain from investing in IT security (Zurich, 2017).

Second, the critical analysis of extant organizational IT security research focuses on the (investment) decision and serves as a magnifying lens that highlights various other important research gaps such as the influence of factors other than economic or organizational aspects, which currently still dominate in many studies. Additionally, our approach is the first to our knowledge that explicitly investigates nuances of investment decisions and the intended audience.

However, in accordance with previous literature review-based and qualitative research, one limitation of this study refers to potential subjectivity during the selection and analysis process. Given the choice of keywords and the screening process of the literature, complete exhaustion or generalizability of the results cannot be claimed. Similarly, qualitative approach through interviews might be affected by the ambiguity of language or a self-selection bias of the interviewees. Nevertheless, we employed several techniques such as triangulation and discussed as well as cross-checked our results with other IS researchers. Against this backdrop, future research could broaden our IT security investment focus and consider other general IT adoptions or determine the respective influence of the identified contextual aspects in companies of various sizes and within several industries. Moreover, our literature analysis shed light on largely overlooked nuances in current IS security investment decisions. We uncovered huge gaps considering sourcing and initial adoption decisions which should receive future attention. Especially, since the latter nuance is highly relevant for the SME context and the stepping stone for further nuances during the decision process.

In general, future IT security research in particular would highly benefit from a more distinct consideration of the mechanics and insights derived from behavioral economics and neuroscience. This is the only way to ensure better integration of context into risk management and IT security decisions.

6.7 Acknowledgments

This work has been co-funded by the BMBF project secUnity “Supporting the Security Community”.

7 Paper D: The Influence of SME Constraints in an Organizational IT Security Context

Title

The Influence of SME Constraints in an Organizational IT Security Context

Authors

- Margareta Heidt, Technische Universität Darmstadt, Germany
- Jin P. Gerlach, Technische Universität Darmstadt, Germany

Publication Outlet

Proceedings of the 39th International Conference on Information Systems (ICIS), San Francisco, USA. VHB-Ranking: **A.**

Abstract

Small and medium-sized enterprises (SME) represent more than 95 percent of all businesses worldwide, yet organizational IT security research has largely neglected SME or superimposed certain theoretical assumptions that are not necessarily applicable in an SME context. Based on a literature review and a resulting conceptualization of general SME characteristics, several constraints are validated and contextualized regarding their influence on IT security investment decisions through 25 expert interviews. The findings strongly suggest that several widely held assumptions in extant IT security literature have to be modified if researchers claim generalizability of their results in an SME context. Exemplary assumptions include the existence of formalized, documented processes or IT budget planning which are often non-existent or underdeveloped in SME. Additionally, our study offers 14 propositions regarding the particular effects of identified constraints on IT security investment decisions in SME for future IT security research.

Keywords

IT Security, SME, Constraints, Investment, Qualitative study

7.1 Introduction

“Digitization without IT security is like bungee jumping without a rope!” – experts in research and practice commonly agree that digital transformation of business and everyday life will only succeed sustainably with effective IT security measures and a heightened IT security awareness

of individuals and executives alike. A considerable stream of research has focused on organizational IT security in leading Information Systems (IS) journals and continues to highlight important legal, technical, procedural, and human aspects in this regard. The immense relevance of organizational IT security is only reinforced by the continued emergence of large-scale attacks on organizations and the ever-increasing damages thereof. Ransomware attacks such as CryptoWall in 2015 or NotPetya in 2017 with an estimated economic damage of 325 million respectively 1 billion USD worldwide (Lemos, 2017) along with the increasing frequency of other security breaches has put a spotlight on the importance of securing IT systems in organizations. This elevated need for IT security measures has reached boardroom agendas and strategies in enterprises worldwide as evidenced by a rise in expenditure in 2017 of 7.6 percent, compared to 2016, reaching 90 billion USD according to research company Gartner (Forni & van der Meulen, 2017).

Despite these visible improvements, recent reports indicate that especially small and medium-sized enterprises (SME) are still slow to invest (Zurich, 2017) albeit seeing themselves as ill-prepared for potential attacks (Kaspersky, 2017). Even more tellingly, almost half (49 percent) of British SME plan to spend less than 1000 GBP on cyber security measures within the upcoming year (Zurich, 2017). The major importance of small and medium-sized enterprises for national economies amplifies the significance of these findings: SME, i.e., enterprises with less than 250 employees represent around 95 percent in OECD countries and even 99 percent in the EU28 states while accounting for 60 to 70 percent of jobs in most countries (e.g., Eurostat, 2015; OECD, 1997). Although their total contribution to the overall gross domestic product is lower than the one of large enterprises, the role of SME as drivers of employment and innovations, and their role as the respective country's backbone is largely agreed upon (e.g., Dutta & Evrard, 1999; Verhees & Meulenberg, 2004).

Surprisingly, there is a dearth of research focusing on organizational IT security in an SME context – in particular within the so-called Basket of Eight which includes the leading IS journals. Studies in this field mostly generalize their results for organizations of all sizes or industries although their samples predominantly feature large enterprises (e.g., Angst et al., 2017; Hsu et al., 2012; Straub & Welke, 1998) or focus on a specific industry sector such as healthcare or finance (e.g., Kwon & Johnson, 2014; Wang et al., 2008). Moreover, they neglect to discuss whether and how their results might be bounded by company size. With the exception of Lee and Larson (2009) who focus on SME executives' organizational adoption of anti-malware software, most studies do not report specific results for SME.

However, several studies within the IS discipline and related disciplines that focus on technology adoption or knowledge management have shown that SME face distinct challenges and particular constraints. Additionally, many of these constraints affect large enterprises only seldom or not at all (e.g., Decker et al., 2006; Riemenschneider et al., 2003). Researchers like Bharati and Chaudhury (2009) have demonstrated that SME differ from large firms in terms of their organizational characteristics as well as their relationship to information systems. Among others, they have criticized the limited space provided for IT aspects of SME in most journals which is highlighted by the identification of only a single article on the subject published between 2003 and 2009 in the top three IS journals in the United States.

Given the significant relevance of the SME context, we advocate that future IS security research needs to take the particular characteristics of SME fully into account. In line with Davison and Martinsons (2016), we argue that extant recommendations stemming from previous studies and their particular context are not necessarily applicable to smaller enterprises. Angst et al. (2017), for example, make the case for substantive adoption of IT security measures that are defined by deep integration into a process and ongoing learning efforts – a recommendation thwarted by the often limited documentation and formalization of organizational processes in SME. Therefore, our paper makes a first step to enable future IS security research in an SME context and investigates the following research questions: (1) *Which SME constraints influence organizational IT security?* And (2) *how do these identified SME constraints manifest themselves and influence IT security (investment) decisions?*

To answer these questions, we first define the term SME and perform a structured literature analysis to identify general constraints that SME face on an organizational level. Subsequently, the quintessence of this literature review is conceptualized into a framework that serves as a lens for the second step. This second step includes a qualitative analysis of 25 semi-structured interviews with a total of 26 decision-makers and IT staff from small to medium-sized client and provider organizations. These interviews are analyzed to validate whether the previously identified general constraints can be applied to the organizational IT security context. Furthermore, the qualitative analysis provides insight into how these constraints manifest themselves specifically in IT security decision-making processes based on the perception of subjects within the SME context. Discussing these manifestations increases our understanding of how specific constraints influence IT security decisions and enables the proposition of several key starting-points for future research regarding organizational IT security in an SME context.

Consequently, our approach entails several important contributions for theory and practice. From a theoretical point of view, our results depict the apparent negligence of leading IS journals in representing the reality of SME in terms of organizational IT security. By highlighting the influence of SME-specific constraints in IT security (investment) decisions, we expose the necessity to expand, rethink, or constrain prevalent theories in organizational IT security research. Additionally, our findings also raise awareness for research gaps within the IT security field such as the tendency to neglect temporal and affective factors or a low procedural sophistication in SME. Practical implications should be considered by both user and provider organizations for IT security products and services. Providers can learn that top executives in SME differ in their decision-making process and draw heavily on emotions and affects while user organizations should take our results as an indication to expand their timeframe and establish formalized and documented processes along with more strategic IS management practices.

7.2 Conceptual Framework

In order to specify and define the concepts associated with the identified research questions, we propose a conceptual framework in line with Miles and Huberman (1994, p. 440) as it "lays out the key factors, constructs, or variables, and presumes relationships among them".

7.2.1 Definition of SME Context

We conducted a literature review to identify those SME-specific constraints that are relevant to IT security decisions and to construct a conceptual framework that can serve as a foundation for further analysis. Drawing on the approach suggested by Levy and Ellis (2006) we followed three steps, i.e. input step, processing step, and output step, for a scoping review that summarizes research findings on SME constraints. During the input step, we conducted a database search (Ebsco Host Business Source Premier, Science Direct, and AIS Electronic Library) and additionally queried Web of Science and Google Scholar. Relevant articles were identified using the following keywords: *(barrier OR constraint OR restraint OR boundar* OR problem OR issue OR challenge OR obstacle OR characteristic) AND (SME OR SMB OR ((small OR medium OR micro) AND enterprise OR company* OR firm))* with "*" as an abbreviation symbol. The search was not limited to a certain time period but focused on highly cited articles. The processing step encompassed title and abstract screening, followed by a screening of the remaining articles for clearly stated constraints that are specific to SME. The resulting final findings were synthesized during the output step which resulted in a conceptual framework of these identified SME constraints.

7.2.2 Identification and Categorization of Constraints

Based on our literature analysis, we identified several environmental factors and constraints which were categorized into characteristics internal to the focal firm and those associated with the firm's (external) environment. In consequence of our focus, the subsequent analysis primarily comprises organizational and individual characteristics within the focal firm.

Individual characteristics, summarized through "leadership" in the framework, are especially relevant in an SME context due to the widespread multitude of role identities as enterprise owners often function additionally as chief executive officer (CEO), managing or IT directors. Additionally, researchers have pointed out the influential role of top managers in SME as they are often the single decision-maker while being responsible for the survival of the enterprise (e.g., Birley, 1982; Thong, 1999; Thong & Yap, 1995). In this regard, many studies in an IT context have pointed out how managerial capacity, attitude towards technology, or lack of awareness affect decision-making and the success of technology adoption (e.g., MacGregor & Vrazalic, 2005).

Resource constraints commonly refer to a shortage of financial assets and knowhow or expertise (e.g., Boyes & Irani, 2003; Thong, 2001). The latter can be a result of high labor costs and a lack of human resources or skilled workforce that affects SME in particular (e.g., Buckley, 1997; MacGregor, 2003). Similarly, limited budget is among the most prominent features in SME research and business decisions like investments or IS adoptions are often strongly affected by financial constraints (Chen et al., 2007).

The *small asset base* represents another and one of the biggest and most cited constraints for SME. This aspect comprises both the difficulties of SME to access external financial resources (e.g., Carbo-Valverde et al., 2007; Riemenschneider et al., 2003) and general cash flow difficulties (Welsh & White, 1981). Additionally, SME capital is often bound to the owners, thus potentially leading to a restricted capacity for strategic, long-term economic risk and investments (Howorth, 2001).

Low formalization level in SME is closely linked to the above-mentioned constraints. It describes the existence of dual or even multiple role-identities ascribed to one individual person, e.g., IT functions and general management tasks are performed by one person due to a shortage of skilled personnel or time. Additionally, CEOs often execute administrative tasks and have to make business decisions while drawing on adhoc, non-formalized, undocumented management practices resulting in a rather low procedural sophistication and highly centralized structures (e.g., Chell et al., 1991; Mintzberg, 1989).

Another organizational characteristic that relates to both internal processes and the micro environment is the cultural and/or geographical *insularity* of SME as stated by Bharati and Chaudhury (2009). They explain that SME are often limited in their interaction with their environment due to their location and generally maintain the most important business relationships with suppliers, partners, and customers in a limited geographical area. This lock-in is further aggravated by an overreliance on strong ties within the closest community which could lead to a preservation or backwardness in terms of business culture and prevents access to other or new information sources (e.g., Agell, 2004; Bennett & Robson, 2004).

These characteristics are depicted in Figure 1 which is loosely based on the IT business value model proposed by Melville et al. (2004) and SME constraints in a general IS context proposed by Bharati and Chaudhury (2009). The aforementioned constraints are closely linked to leadership, have an impact on each other, and are further influenced by the respective micro and macro environment of the focal SME (e.g., Chell et al., 1991; MacGregor & Vrazalic, 2005). These environments comprise country characteristics like legal regulations or general globalization pressures which are not necessarily specific to the SME context but affect smaller companies to a greater extent compared to large enterprises (e.g., Chen et al., 2007; Piscitello & Sgobbi, 2004). The micro-environment is the direct periphery of the SME, i.e., competitors, suppliers/providers, customers and general industry-specific characteristics which affect the enterprise through market pressures (e.g., Melville et al., 2004; Stockdale & Standing, 2006; Teo et al., 2004). For instance, SME are particularly pressured due to their position at the end of the value chain, as evidenced by "auditing chains" and are typically regarded as price-takers (Casterella et al., 2004). These pressures of the micro and macro environment are not of central interest in this study and will thus not be investigated further but are mentioned and depicted for the sake of completeness. The following qualitative study focuses on organizational and individual constraints of the focal SME (i.e., inner "Focal SME" box in Figure 12).

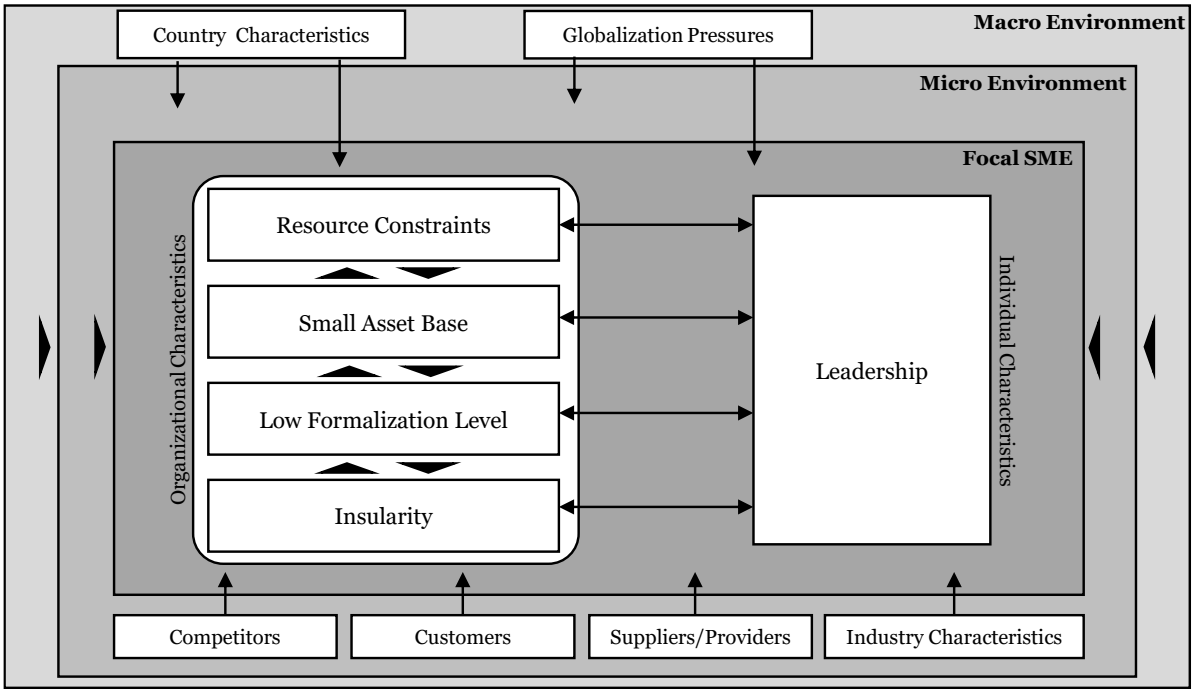

Figure 12. Conceptual Framework of SME Constraints

The conceptual framework represents the base for the following contextualization of constraints regarding organizational IT security in SME. Subsequently, their relevance and influence on IT security (investment) decisions will be identified via a qualitative research approach (Ravitch & Riggan, 2016).

7.3 Qualitative Research Methodology

After the deliberate consideration of the findings from our initial literature analysis on the specific SME constraints, a qualitative approach was employed to validate and contextualize the findings within organizational IT security. Following Kaplan and Maxwell (1994), we argue that it is important to understand the perceived boundaries and constraints from the point of view of participants in that particular social and institutional context – in our case relevant decision-makers in SME user and provider firms. Whereas the dominant stream of IT security literature employs quantitative research methods, we argue that certain covert assumptions or preconceptions might be irrelevant or incongruous for the SME context. In order to challenge these assumptions, we advocate for the necessity to "see the world through the eyes of the actors doing the acting" (Greener, 2008, p. 17), i.e., employing a qualitative approach using interviews with experts within that particular context. As our approach is based on a conceptual framework, thus relying on stated knowledge but still embraces the skepticism innate to interpretivist

approaches, an epistemological post-positivist stance allows for a more comprehensive explanation of the context of the studied phenomenon (Fischer, 1998). Our approach sets out to broaden the current state of IS research in organizational IT security in SME by questioning experts – both from the perspective of IT staff and executives from user and provider organizations.

7.3.1 Research Design

Our research design adheres to guiding principles of Sarker et al. (2013). Following these guidelines, we prepared an interview protocol resulting in semi-structured interviews with key informants in different organizations. In order to overcome typical pitfalls of semi-structured interviews like the artificiality of the interview or lack of trust, we followed Goffman's recommendation of seeing the qualitative interview as a drama with a stage, props, actors, an audience, a script, and the actual performance (Goffman, 1959). Especially, first impressions are seen as crucial for the success of the interview. Hence, email and telephone contact was used prior to the interview and the actor, i.e., the interviewer, showed empathy and understanding to decrease the chances of the interview going awry (Hermanns, 2004). The initial script itself included several strategies regarding the type of questions asked, e.g., meaning questions to evoke previous experiences with IT security measures and decisions, process questions to identify a longitudinal change regarding IT security, or descriptive questions aimed at identifying underlying beliefs and practices of the investigated social group (Morse, 1994). Additionally, provocative or ideal questions were posed in order to elicit perceived constraints (e.g., "In your opinion, what would be necessary to achieve an ideal status quo of organizational IT security in your company and in other SME?"). Due to the semi-structured approach, initial questions were subject to change and adapted to the respective interview partners and their position or knowledge throughout the interviewing process.

7.3.2 Sample and Data Collection

From November 2017 until February 2018, CEOs or owners and IT executives of SME in Germany were identified via an online social business network and the local Chamber of Industry and Commerce. The invited interview partners were chosen in a key informant approach from user firms (UF), user and provider firms (UPF), and later on also from provider firms (PF). This distinction is based mostly on the product or services portfolio of the respective firm employing our interview partners. While UF are purely clients of IT security services and products, PF are

mainly suppliers of such goods, and UPF introduced security services or products recently to diversify their established portfolio.

In order to avoid an elite bias both IT staff and executives were invited (Miles & Huberman, 1994). Due to the semi-structured approach and additionally derived insights from interview partners, executives and staff from IT security providers were additionally invited to participate. While most interviews were held face-to-face because of the rather intricate and sensitive nature of the topic, a total of seven interviews were performed via phone calls due to geographical distance. Seven interview partners identified themselves with a pure IT role, while two held a hybrid position and 13 were top executives and managing directors (MD). Another four interview partners were either responsible for sales or consultancy. Only one of the interview partners was female. The majority of participants (60 percent) were active in the service sector while 24 percent of the sample organizations provide a mixture of services and manufactured goods, eight percent each are either focusing on production or trade. The self-stated role(s) of the interview partners and their respective experience (Job Exp.) in their role as well as their companies' classification of economic activity according to the ISIC classification, the specific sector and size are depicted in Table 1. All interviews (length average of 72 minutes) were recorded and transcribed by mutual agreement and enriched by field notes by the researchers. All interviewees were guaranteed anonymity and offered an executive report of the results. No additional interviews were scheduled after the 25th interview because further contribution through additional qualitative data to a concept or a relationship between concepts was deemed unlikely after the fifth provider was interviewed (i.e., theoretical saturation was assumed). This quantity of interviews is comparable to other organizational IS (security) publications (e.g., Marshall et al., 2013; Sonnenschein et al., 2017).

ID	Position	Job Exp.	Other Responsibilities	ISIC	Firm's Sector	Size	Interview Method
Group: User Firm (UF): Key informants of firms that are solely users of IT security products and services							
UF-01	Director IT	19 years	-	C	Chemical Manufacturing	m	Face-to-face
UF-02	MD	10 years	IT Administrator	M	Marketing Services	vs	Face-to-face
UF-03	CIO	40 years	-	P	Educational Services	m	Face-to-face
UF-04	MD Director IT	22 years 20 years	Owner -	C	Mechanical Engineering	m	Face-to-face
UF-05	MD	20 years	IT Administrator	M	Legal Services	s	Face-to-face
UF-06	MD	12 years	IT Administrator	F	Building Reconstruction	s	Face-to-face
UF-07	MD	5 years	IT Administrator	M	Marketing Services	vs	Telephone
UF-08	Director IT	7 years	-	G	Retail	m	Face-to-face
UF-09	MD	10 years	IT Administrator	N	HR Services	s	Face-to-face
UF-10	MD	4 years	Sales Manager	M	Marketing Services	m	Telephone
UF-11	Director IT	18 years	-	G	Wholesale	s	Telephone
UF-12	MD	10 years	Sales Manager	M	Marketing Services	s	Face-to-face
UF-13	MD	8 years	Consultant	M	Consultancy	s	Face-to-face
UF-14	MD	4 years	Consultant	M	Consultancy	vs	Face-to-face
UF-15	Director IT	5 years	Project Manager	P	Educational Services	s	Face-to-face
UF-16	Consultant	6 years	IT Administrator	J	IT Project Management	s	Face-to-face
UF-17	MD	2 years	IT Administrator	M	Legal Services	vs	Face-to-face
UF-18	CIO	20 years	-	N	Relocation Services	s	Face-to-face
Group: User and Provider Firm (UPF): Key informants of firms that are both users and providers of IT security products and services							
UPF-01	MD	10 years	CIO	J	Publishing and IT Services	s	Face-to-face
UPF-02	Director IT	20 years	-	J	Publishing and IT Services	m	Face-to-face
Group: Provider Firm (PF): Key informants of firms that are providers of IT security products and services							
PF-01	Sales	5 years	Consultant	J,M	IT Services	s	Face-to-face
PF-02	MD	21 years	-	J,M	IT Services	s	Telephone
PF-03	Consultant	19 years	-	J,M	IT Services	m	Telephone
PF-04	Sales	2 years	Consultant	J,M	IT Services	m	Telephone
PF-05	MD	20 years	-	J,M	IT Services	s	Telephone

ISIC Codes (United Nations 2008): C= Manufacturing; F= Construction; G= Wholesale and Retail Trade; J= Information and Communication; M= Professional, Scientific and technical Activities; N= Administrative and Support Service Activities; P= Education;
Firm Size: vs= very small; s=small; m=medium

Table 11. Participant Overview

7.3.3 Data Analysis Technique, Coding Concept and Criteria for Rigor

In line with the philosophical stance and the developed conceptual framework, the transcripts were analyzed using an iterative multi-level coding process similar to extant IS literature (Albrechtsen, 2007). Coding cycles were used to answer our research questions as displayed in Figure 2 following the suggested techniques of Miles and colleagues (2013).

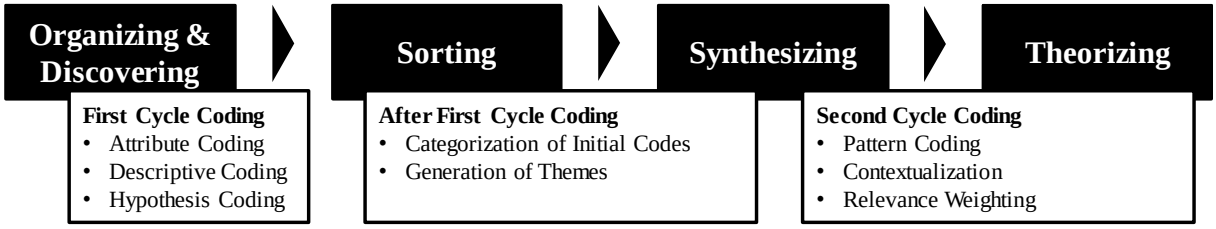

Figure 13. Analysis Technique and Coding Concept (Miles et al. 2013)

After an initial familiarization with the transcripts and simultaneous memoing, the methods if the first cycle coding consisted of attribute, descriptive and hypotheses coding using MAXQDA

software to facilitate the analysis process (Bazeley, 2003). *Attribute* coding or context coding was used to identify essential information about the data at hand and demographic characteristics – for example, age, gender, experience, position, time frame – resulting in an overview of the sample (see table 1) and in a potential attribute base used to expose interrelationships or themes in a later coding stage (Bogdan & Biklen, 2007). Furthermore, *descriptive* coding was employed to summarize topics resulting in a general categorized code inventory which provided a basis for additional, more focused analysis and interpretation (Wolcott, 1994). This coding technique was primarily used to possibly extend the initially developed conceptual framework by disregarding the previously identified constraint dimensions (i.e., limited resources, low formalization level, insularity, asset base, and leadership). Descriptive coding was mainly employed to identify further potential constraints and their manifestations. As recommended by Saldaña (2009) *hypothesis* coding was performed subsequently to account for the initially conceptualized constraints and to screen the scripts for verbatim and in spirit mentions (Auerbach & Silverstein, 2003). For example, statements regarding the resource situation were further analyzed and broken down into themes, e.g., specific resource aspects like budget or time. The first coding cycle thus helped to gain a general and broad overview by identifying relevant themes regarding IT security investments. Subsequently, resulting initial codes were once again categorized into themes, i.e., the distinct manifestations of the aforementioned constraint dimensions during the sorting and synthesizing steps. These themes were further analyzed during the second cycle through pattern coding, contextualization, and relevance weighting which served as a lens to examine further patterns or explanations for the subsequent theorizing stage (Miles & Huberman, 1994). Relevance weighting was considered by extracting the exact code frequencies and analyzing the summary grid of codes through MAXQDA's analysis features. The relevance had been considered based the overall frequency of mentions per interviewee role (MD, IT, or other) subdivided into user and provider firms (UF and UPF) and pure provider firms (PF). Subsequently, visual tools offered by MAXQDA that examine and visually illustrate frequency measures were assessed and resulted in the following weighting scheme: ■ = very high relevance; ▣ = high relevance; ⊡ = low to medium relevance; and □ = no or very low relevance.

Several practices were employed throughout the coding and analysis process in order to achieve rigor and trustworthiness: The data analysis was led by clear research questions and prior theorizing served as the base of the conceptual framework and was used as input to our research design. In terms of the selected interviewees, a broad range of highly involved individuals

across several industries enable extensive comparisons and potentially yield more general research results (Benbasat et al., 1987). Furthermore, the data collection was supported by data triangulation by including both user and providers of IT security measures while field notes and a multi-researcher triangulation was employed during data analysis. Other tactics, as proposed by Miles and colleagues (2013) included weighting the evidence to identify the most trustable data and to pay attention to "unpatterns" by checking for outliers, extreme cases, and negative evidence. Furthermore, the following presentation of findings including direct quotes brings "the voice of participants in the study" (Creswell, 1998, p. 70), while contributing to transparency and accountability.

7.4 Results

The identified SME constraints (see Figure 1) were validated in differing degrees as interviewees perceived certain constraints as more relevant or severe in their specific environment. Table 2 includes the weighted perceived relevance according to the interviewee's role within the organization, as we noticed distinct patterns among managing or IT directors in user firms and among interviewees from provider firms. A general overview of these relevance ratings and manifestations can be extracted from the following table which is followed by a demonstration of manifestations through concrete interviewee statements.

General Constraint	**Constraint Aspects**	**Constraint Manifestation**	**Effects on Organizational IT Security**	**Weighting per Role and Firm Group**		
				MD UF, UPF	**IT** UF, UPF	**MD, other** PF
Limited Resources	Limited Budget	No or limited budget for IT security investments	→ less expenditure for IT in general and IT security in particular	■	▣	▣
	Limited Time	No or limited time for discussions, information search regarding IT security investments	→ less expenditure for IT in general and IT security in particular	■	▣	■
	Limited Knowhow	No or few experienced employees to assess IT security (investments)	→ negative impact on expenditure regarding IT security	■	⊡	⊡
Small Asset Base	Revenue Stream	Cash flow difficulties or irregularities affect IT security investments	→ hindrance for further IT security investments	⊡	⊡	⊡
	Financial Support	Difficulties to obtain financing through institutions or government	→ no distinct influence on IT security investments	⊡	⊡	⊡
	Owner Capital	Firm assets are directly linked to owner's personal assets and (IT) investments assessed differently	→ marginal influence on IT security investments	⊡	⊡	⊡
Low Formalization Level	Budget Planning	No or marginal budget planning for IT and IT security in particular	→ negative impact on expenditure regarding IT security	⊡	▣	■
	Multiple Roles	Multiple roles and responsibilities within one position and non-existent IT department	→ non-accountability/ no defined authority for IT security issues	⊡	▣	▣
	Processes	Non-existent, undefined, or undocumented (organizational, technological) processes	→ negative impact on expenditure regarding IT security	□	⊡	■
Insularity	Geography/ Location	(Rural) location restricts sourcing of IT security products and services	→ limitation regarding IT security experts, products, and service portfolio	▣	⊡	□

General Constraint	Constraint Aspects	Constraint Manifestation	Effects on Organizational IT Security	Weighting per Role and Firm Group		
				MD UF, UPF	**IT** UF, UPF	**MD, other** PF
	Culture	• Cultural insularity emphasizes trust-based relationship	→ personal contact and lengthy commercial partnerships necessary for decision-making	⊡	⊡	▣
		• Ingrained tradition leads to overreliance on status quo	→ overreliance on the status quo of IT in general and IT security in particular	□	⊡	▣
Leadership	Awareness	Lack of awareness or underestimation of IT security risks	→ impedes IT security decision-making and investments	⊡	■	■
	Temporal Focus	Focus on short-term daily business rather than IT security issues	→ limits long-term investments in IT security	▣	⊡	■
	Affective/ Experiential Factors	(Over-)Reliance on emotional factors in decision-making	→ overall negative impact on IT security decision	▣	▣	⊡

■ = Very high relevance; ▣= high relevance; ⊡ = low to medium relevance; □ = no or very low relevance
UF = User Firm, **UPF** = User and Provider Firm; **PF** = Provider Firm

Table 12. Findings: Manifestations of Constraints and Relevance Weighting

While manifestations of limited resources and leadership constraints were most prevalent and deemed relevant unanimously, insularity or small asset base received differing support. The latter two constraint manifestations were mentioned more often by MDs of user firms. In contrast, manifestations of low formalization level and insularity (excluding geographical insularity) received more attention and higher relevance ratings by IT executives of user firms and interviewees from provider firms. In the following, we provide more detailed findings on how general constraints of SME manifest themselves in an IT security context.

7.4.1 Limited Resources

Limited resources were among the constraints most often mentioned by all interviewees across firms and positions. The manifestations of these constraints in an organizational IT security context refer especially to limited budget, time, and workforce which are all highly interrelated but influence IT security investments in a distinct manner as illustrated in the following.

Limited financial resources were mentioned most frequently by managing directors and very often by IT staff and interviewees from provider firms in line with a multitude of SME studies. Especially, owners and managers of smaller businesses see IT security investments as a strong cut into their finances. Also, when asked how they see their own company's organizational IT security status compared to larger companies, managing directors often attribute a better status in large companies to the available financial resources. The influence of limited budget is evidenced by the following statement:

> "I mean, I did try to inform myself about it and the smallest server we'd need costs 4000€! Well yes, 4000€ is a lot of money!" – UF-02, Managing Director

Limited Time was one of the most frequently stated constraints in the sample. Especially, managing directors pointed out that security issues require a lot of time for them personally but also across the whole organization. Specifically, statements regarding time often included the phrase "I have to take/make time". Dealing with IT security and decisions regarding the investment in IT security measures are generally seen as extra tasks that can be performed only by cutting time expenditure on other organizational tasks. These statements are also intertwined with manifestations of low formalization levels regarding multiple roles and responsibilities within one position. This perspective is also shared by interviewees from provider companies and IT executives in user companies:

> "[IT security as a topic] is something you have to research a lot to learn the ropes, to familiarize yourself. If we actually think about implementing a solution that is recommended, it can become too time-consuming for us. In some cases, it might be better to attend trainings but that is something a fulltime IT administrator could do […]." - UF-16, Consultant in a user firm who is responsible for IT administration

Limited knowhow was mentioned frequently by all interviewees and strongly intertwined with the aforementioned resource constraints. This constraint manifests itself in two particular ways: (1) SME do not have any specialized IT personnel with enough knowhow regarding IT security or (2) the IT personnel is already fully stretched and cannot be involved in IT security projects. The latter option was brought forward especially by interviewees with an IT background. Managing directors often mentioned a general shortage of skilled IT workers and lacking knowhow intertwined with awareness regarding IT security in SME altogether:

> "Well, I would say that SME do not care enough or at all to actually deal with IT security issues, because – I think – there are no employees with enough knowhow regarding IT", UF-09, Managing Director

In line with these constraint manifestations, we formulate the following propositions:

> ***Proposition 1****: Limited financial resources will have a negative effect on IT security investments in SME*
>
> ***Proposition 2****: Limited time dedicated to IT security questions of decision-makers in an SME will have a negative effect on IT security investments in SME*
>
> ***Proposition 3****: Lack of IT staff or overall lack of IT knowledge and expertise in SME will have a negative effect on IT security investments in SME.*

7.4.2 Small Asset Base

A small asset base was one of the less prominent constraints mentioned by all interviewees. However, we could still find evidence that a small or irregular ***revenue stream*** affects IT security investments:

> "And especially small or medium-sized startups do not have a current revenue, so there is no money left for IT security spending." – UF-15, CIO

Even though the initial literature review on SME constraints stresses the difficulty to obtain external ***financial support***, some interviewees actually expressed that funding and subsidies are readily available whereas a few managing directors pointed out the difficulty to obtain certain grants or the ignorance of their existence altogether. No interviewee mentioned that they had ever drawn on external financial support for any IT security investment decision so a distinct influence of this constraint could not be established. Limited support for this constraint is evidenced by the following statement:

> "There are a couple of good loans that are available and one should debate whether it is truly necessary to finance an investment always via the one's own cash flow or if it is possible to get some [external] support. […]. There certainly are very attractive schemes – it's only that no one knows about them." – UF-12, CIO

As for ***owner capital***, interviewees who were the actual owners mentioned sporadically that any decision regarding IT security investment required them to draw on their personal capital. IT directors and providers indirectly regarded this constraint manifestation as a possible hindrance for further investments arguing that the actual "value" or return on investment has to be explicated in more detail if the owner has to spend his/her own money on something as intangible as IT security measures.

> "This actually means that I don't have the financial means, if I don't reach deeper into my own pockets and say: 'I'll pay someone ten to twenty thousand Euro in a lump sum'. I think this is true for the majority of companies [SME]" – UF-07, Managing Director

Constraints resulting from the small asset base will hence influence IT security investment as follows:

> ***Proposition 4****: Irregular revenue streams will have a negative effect on IT security investments in SME*
>
> ***Proposition 5****: External financial support will have no or an only marginal effect on IT security investments in SME*

***Proposition 6**: The owner's own capital will have no or an only marginal effect on IT security investments in SME.*

7.4.3 Low Formalization Level

A lack of infrastructure, strategic planning, or processes are a common theme when discussing SME constraints in general. Against the backdrop of IT security, three themes emerged frequently, namely ***budget planning*** (or the lack thereof), multiple roles or responsibilities within one position, and undocumented processes which will negatively impact IT security investment.

When asked about possible hindrances to IT security investment, IT staff and providers mentioned a lack of budget planning as being a factor. Likewise, some managing directors admitted that they do not have a structured budget planning process in general or for IT (security) spending in particular.

> "It [budget planning] does exist of course but is a glorious exception in my professional experience! In most companies, it'll go according to the motto "if we need it, we need it" – PF-05, Managing Director

As mentioned earlier, limited time can be both seen as consequence and reason for the existence of ***multiple roles and responsibilities within one position***. This understaffing is a common feature in SME and their management of information systems as illustrated by West (1975) who states that, "almost without exception, the small company is grossly understaffed, often being a one-man operation." As already illustrated in our sample table (table 1), many managing directors are also responsible for IT and IT security issues while some IT administrators also have to cope with several roles and responsibilities other than usual administrative tasks like setting up new devices for colleagues or new programs. In this regard, both managing directors and IT staff mentioned the plethora of tasks that are of higher priority resulting in IT security being a topic that is often neglected and followed up with the sole goal of not causing too much damage:

> "Like I mentioned, the only thing you can try to do is avoid acting grossly negligent. My problem is honestly that given the many things I have to do every day, and all the issues that keep on bombarding me… well I would like to act rather react all the time. But that is truly difficult." – UPF-01, Managing Director

The last manifestation of a low formalization level are ***non-existent, undefined or undocumented (organizational and technological) processes*** paired with "adhoc" decision-making.

This was most commonly expressed and deemed highly relevant by provider companies and experienced IT personnel. Especially, interviewees of provider companies saw an additional problem in unawareness of top managers in SME for the necessity of documented organizational and technological processes. Especially, documentation in smaller companies is not continuously performed which complicates the service of providers who need to invest considerable time and effort into comprehending the actual IT architecture before actual measures can be implemented. Also, especially IT directors in medium-sized companies pointed out that they had to assess all existing processes and structures for the first time within their company which confirms the assumption of low procedural sophistication in SME.

> "In many cases, you will find organically grown structures that are clear to no one. Someone has put a storage here, someone has done something else there. Sometimes companies have double storage but they don't even know about the existence of both!" – PF-01, Business Development

We thus posit that the low formalization level and procedural sophistication affects IT security as follows:

> ***Proposition 7****: Non-existing or rudimental budget-planning regarding IT and IT security will have a negative effect on IT security investments in SME*
>
> ***Proposition 8****: Individuals who are responsible for multiple tasks – besides IT – are less capable or willing to consider IT security questions resulting in a negative effect on IT security investments in SME*
>
> ***Proposition 9****: Ill-defined or undocumented organizational and technological processes will have a negative effect on IT security investments in SME*

7.4.4 Insularity

Geographical insularity as a constraint was mentioned in two regards of sourcing: namely sourcing of personnel and service providers. Especially, SME with a more rural location experienced difficulties to attract IT personnel. Furthermore, physical remoteness and thus isolation from providers was seen negatively as it limits sourcing and vendor options. The few experts in rural areas are often fully booked and cannot assist SME regarding IT security decisions, especially if new regulations like the GDPR require many firms to act and invest in external IT security specialists as evidenced by the following statement:

> "Well, I just talked to the guy who helped us set up our computers and works in an IT firm. He said 'Pff, you can already try to make an appointment with me now because I'll be completely booked

> out until then' […] and additionally I don't really know whether there are enough IT people who can actually sell and install things. Not here in this area at least." – UF-02, Managing Director

Culture in terms of cultural insularity, trust-based relationships, and ingrained traditions was a constraint often emphasized by providers. Both interviewees from user and provider companies pointed out that trust was extremely important both between IT director and managing director as well as between the decision-maker within the user company and the external partner in a provider company. Additionally, trust plays an important role in the information search process as decision-makers often draw on the expertise of a trustee in their personal network rather than solely on provider recommendations. Trust with providers can only be established through increased personal contact and lengthy or even historical partnerships.

> "[…] I need to be informed from someone I trust. When I talk to a colleague [CIO in a different company] and you hear 'I've used this and it didn't help at all' than I can assess it better than if a provider tells me that." – UF-11, CIO

On the other hand, many providers also attributed the lack of IT security investments to the traditional mindset and overemphasis on the status quo in SME. According to one interviewee, critical assessments of the IT security status quo and subsequent recommendations are even seen as an attack on the user company's self-perception:

"In most SME, they don't really have anything [IT security measures] and if we make them aware of this, we are actually the bad guys from their point of view. Because they live in an idyllic world and they don't really want to know about." – PF-02, Managing Director

> ***Proposition 10****: A rural location impedes IT security sourcing and will have a negative effect on IT security investments in SME*
>
> ***Proposition 11****: Trust will influence IT security investment decisions positively whereas an overreliance on the status quo will have a negative effect on IT security investments in SME*

7.4.5 Leadership

The substantial and highly influential role of top management or leadership in SME has been widely discussed and highlighted in general SME research and was validated during the interviews. Most interviewees agree that the management style or the personality of the managing director or owner have a profound effect on IT security decisions.

Managing directors themselves attribute a lot of underinvestment in IT security to the prevalent ***lack of awareness*** regarding IT security in general. IT directors and providers regard awareness in the top management as an important prerequisite for the overall awareness in a company.

> "This topic 'raising awareness' is located right at the heart of leadership. Only if they nod, it transcends top-down within the company and you can actually implement it [IT security measures] in the whole company." – PF02, Managing Director

However, awareness alone or lack thereof is not the only frequently mentioned leadership constraint. Especially providers explained underinvestment with the ***temporal focus of leadership*** on short-term daily business. They state that decision-makers in SME rather focus on short-term success and neglect long-term risks for their organizational IT security due to a lack or the neglect of strategic planning:

> "Strictly speaking it's a matter of priorities. I think the priority in SME as of now is on the day-to-day operations, on satisfying the demand. Simply to keep the daily business running."– PF-04, Business Development

Admittedly, short-term focus plays a significant role in postponing decisions regarding IT security investments. Nevertheless, both interviewees in user and provider companies acknowledge that the highly complex nature of IT security needs to be accounted for. In this line, several managing directors and some CIOs mentioned that they rely heavily on their "gut feeling" due to the lack of information, knowhow, and time for decisions. This demonstrates that decision-makers draw on ***affective and experiential factors*** in IT security investment decisions in addition to or rather than on economic modelling or formalized decision support systems.

> "You obviously try to calculate the RoI [Return on Investment] but you can easily come up with nice target figures so I consider it rather 'relative'. This is certainly very important in big enterprises […] It is admittedly not easy to calculate such numbers in the area of security. We do have a decision matrix that we use as an orientation. So, it is not a pure gut decision but I have to say that gut feeling does play a certain role by now. We have hands-on experience with several providers and both play an important role. But we don't have a further formalized decision system." – UPF-02, CIO

Unsurprisingly, leadership characteristics influence decisions regarding organizational IT security in SME strongly. Hence, we posit:

> ***Proposition 12****: Lack of awareness will be more pronounced in SME and will have a negative effect on IT security investments in SME*

Proposition 13*: A short-term temporal focus is more prevalent across SME and will have a negative effect on IT security investments in SME*

Proposition 14*: Affects and emotions play a pronounced role in IT security investment decisions and will have an effect on IT security investments in SME*

7.5 Discussion of Findings, Limitations, and Future Research

The present paper identified and described relevant SME constraints in an organizational IT security context and examined how these constraints influence decisions regarding IT security investments in SME. Our findings provide several theoretical contributions and practical implications.

From a theoretical perspective, our study validates and contextualizes general SME constraints in organizational IT security and adds to the still prevalent scarcity of qualitative data sources in IS security research. The findings derived from this approach question a variety of assumptions commonly made by studies that deal with SME as "little big firms". The identified and described constraints help define necessary boundary conditions for future research by challenging and modifying prevalent scholarly explanations (Alvesson & Sandberg, 2011; Rivard, 2014). For instance, common assumptions like the existence of dedicated personnel and formalized processes can even be denied for a large share of organizations which should be considered by future organizational IT security studies. Overall, the most overlooked or underrepresented assumptions in extant IT security research concern SME constraints of low formalization, insularity, and leadership.

With respect to low formalization levels in SME, Hsu and colleagues suggest that "technologies alone may not be sufficient to ensure the successful assimilation of a particular innovation, especially an administrative innovation such as information security management" (Hsu et al., 2012, p. 934). Despite their suggestion, a considerable share of studies still implicitly assume the existence of dedicated IT personnel responsible for IT security management (e.g., Straub & Welke, 1998; Wang et al., 2008) or the existence of defined business processes or organizational control frameworks (e.g., Yue & Cakanyildirim, 2007). These assumptions are in direct opposition to the manifestations of low formalization in the SME context. Firstly, our study shows that SME often do not have dedicated personnel but several roles and responsibilities are performed by one individual which aggravates the already mentioned general shortage of time but can additionally lead to a certain lack of accountability and authority for IT security questions in particular. This, in turn, is a consequence of a rather high degree of ambiguity due to

poorly defined job descriptions and responsibilities (Kets De Vries, 1995). Secondly, even though some studies – among them the only SME-specific study in the so-called Basket of Eight – actually find that IT budget influences actual adoption within the non-IT intensive industry (Lee & Larsen, 2009) the actual operationalization of "IT budget" simply considers annual IT spending during the last or current year and does not inquire whether budget planning is actually taking place. Drawing on our results however, especially providers – and to a lesser degree also IT personnel – attribute non- or underinvestment in organizational IT security to inexistent or insufficient actual budgeting within SME and non-existent or undocumented processes as a third manifestation of the low formalization constraint. Even Lee and Larson readily admit that they "did not fully examine the effects of SMB characteristic variables" and that their study is based on the assumption of subjects that are aware of an IT security threat and the effectiveness of the countermeasure (Lee & Larsen, 2009, p. 185).

Further, our study emphasizes the overall insularity of SME both in terms of location and culture. Whereas culture, trust, and ingrained traditions have received attention in IS security research and their effect on management has been widely demonstrated (Van Niekerk & Von Solms, 2010), the potential negative influence of geographical insularity due to a remote or rural location has not been analyzed thoroughly yet even though our findings indicate that SME are likely affected by this constraint. Whereas especially owners and managers point out the difficulties to find adequate IT security solutions due to their sometimes remote location, providers rather indicate that culture in terms of ingrained, often old-fashioned, business traditions inhibits investment. It is apparent in this regard that many studies point out the necessity to investigate these factors when discussing the limitations of their study (Angst et al., 2017; Gordon et al., 2010; Hsu et al., 2012; Hsu, 2009; Hu et al., 2007; Kwon & Johnson, 2014).

With respect to leadership constraints of SME, our results suggest a short-term focus of the leadership due to the eminent trade-off between daily business activities and IT security investments. This trade-off and temporal focus are often disregarded by studies that measure the mere intention to invest in IT security through a "snapshot" i.e. non-longitudinal approach in most experimental or empirical studies as highlighted by Crossler and colleagues (2013). In line with Crossler et al. (2013) and backed by the interview results, we find evidence that even managing directors that are aware of IT security risks and express a general intention towards investing in organizational IT security, will likely prioritize day-to-day business over investments due to their short-term or operational focus. Despite the existence of studies that found a considerable influence of temporal factors in an IT security context, for example regarding organizational

learning and awareness processes (e.g., Jaeger et al., 2017; Mattia & Dhillon, 2003), the influence of a short-term focus in organizational IT security decisions has been largely overlooked. Other leadership constraints such as awareness of top management were validated in the SME context and might even play a more substantial role compared to bigger companies where top management is required to invest in IT security measures due to regulative pressures. Closely linked to awareness is the perception and assessment of IT security risks. We found evidence that these risks are often assessed differently and risk assessment is not as formalized in SME as it is in large enterprises. Specifically, affective and experiential factors influence decision-making processes regarding IT security providers and measures. However, extant organizational literature often draws on game theoretic or resourced-based views and thus neglects non-deliberative or non-analytical risk assessments which likely play a (more) prominent role in the SME context (e.g., Cavusoglu et al., 2008; Weishäupl et al., 2015).

Finally, limited resources have generally received ample attention in current studies. Constraints regarding budget or the expertise, IT skills, or capabilities are regularly discussed and considered influential in organizational IT security (e.g., Hui et al., 2012; Lee et al., 2013). Nevertheless, time as a resource remains often overlooked in decision-making, is equated with measures of effort, or considered only indirectly through response costs due to the difficult operationalization of time aspects (Herath & Herath, 2008). Our results however, across all roles and firm groups, have indicated that limited time affects decisions regarding IT security investments profoundly and should thus be similarly assessed like budget or capabilities.

Our findings thus serve as a magnifying glass that exposes non-generalizable assumptions in extant IT security literature and additionally provide guidelines for future research through the analysis of the inferred propositions. These propositions and associated arguments can be seen as a Type II Theory of Explanation (Gregor, 2006) explicating how and why certain constraints influence IT security decisions in SME. Whereas a dominant stream in IT security literature draws on normative decision theories and models like the Return on (Security) Investment or decision theory (e.g., Cavusoglu et al., 2008), a descriptive approach that takes into account the manifold influencing factors, e.g., available time or geographical insularity, is likely a better lens for organizational IT security decisions in SME. In this regard, we contribute to the rather scarce literature on executive and managerial decision-making in an IT security context by pointing out the influence of individual characteristics – which is possibly highly influential in SME. In addition to the often analyzed lack of awareness (e.g., Hu et al., 2007; Straub & Welke, 1998), the degree of influence and mode of function of temporal, experiential, and affective

factors in IT security related decision-making should be included in order to further advance our understanding of (under-) investment in SME. Furthermore, other propositions concerning insularity or the small asset base could contribute to exposing neglected or inflated effects in IT security investment decisions and thus contribute to both theory and practice.

Through the juxtaposition of decision-makers and employees responsible for IT in user companies and IT security providers our approach also yielded in several practical implications. By contrasting statements, executives should question themselves whether they overemphasize resource constraints such as limited budget as an "excuse" to delay IT security measures. Even though internal IT staff and providers often acknowledge the existence of resource constraints, they rather contribute a lot of underinvestment to low formalization levels and non-existent budget planning which is an indirect result of prioritizing daily business and the short-term temporal focus of managing directors. Executives in SME can thus learn from our findings that documentation and formalization of processes is a first step that might be time-consuming at first but eases the processes of decision-making and leads to fruitful and business-sustaining investments in the long run. Our results also offer several takeaways for providers such as the importance of lengthy discussions to establish trust-based relationships and the influential role of affective and experiential factors in decision-making processes of their potential customers.

This study is not without limitations. First, although we employed measures such as data, subject, and researcher triangulation, qualitative research can still be affected by the ambiguity of language or the existence of an elite bias (Fontana & Frey, 2000). Second, SME should not be considered a homogenous group, especially differences between enterprises in the manufacturing or services have already been noted and discussed. Similarly, very small, small and medium-sized enterprises are possibly affected by the identified constraints to a varying degree. The proposed constraints and their influence in IT security investment should rather be seen on a continuum influencing SME depending on organizational size or industry. Furthermore, our results might be affected by our sample choice as our interviewees are all based in Germany. However, previous organizational SME research has shown comparable patterns of SME characteristics and constraints across national borders and cultures (Chen et al., 2007; Dutta & Evrard, 1999; Thong, 2001). Nevertheless, future research could build on our findings with an international comparison utilizing quantitative measures to determine the effect size of SME constraints on IT security decisions. Additionally, prospective studies should analyze industries

other than healthcare and financial institutions as many of the extant results are hardly generalizable and test the postulated propositions in both an SME and a large enterprise context for more nuanced findings and recommendations.

8 Paper E: Investigating the Security Divide between SME and Large Companies

Title

Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments.

Authors

- Margareta Heidt, Technische Universität Darmstadt, Germany
- Jin P. Gerlach, Technische Universität Darmstadt, Germany
- Peter Buxmann, Technische Universität Darmstadt, Germany

Publication Outlet

Information Systems Frontiers, 21, pp. 1285–1305 (2019). VHB-Ranking: **B.**

Abstract

Lagging IT security investments in small and medium-sized enterprises (SME) point towards a security divide between SME and large enterprises, yet our structured literature review shows that organizational IT security research has largely neglected the SME context. In an effort to expose reasons for this divide, we build on extant research to conceptualize SME-specific characteristics in a framework and suggest propositions regarding their influence on IT security investments. Based on 25 expert interviews, emerging constraints are investigated and validated. Our findings imply that several widely held assumptions in extant IT security literature should be modified if researchers claim generalizability of their results in an SME context. Exemplary assumptions include the presence of skilled workforce, documented processes or IT-budget planning which are often un(der)developed in SME. Additionally, our study offers context-specific insights regarding particular effects of identified constraints on IT security investments for all involved stakeholders (researchers, SME, large enterprises, governments).

Keywords

IT Security, SME, Constraints, Investment, Qualitative Study

8.1 Introduction

'Fuzzy, Irrelevant, Pretentious' – twenty years ago, Benbasat and Zmud (1999) used this proclamation by the Business Week (1990) to analyze "why most IS [information systems] academic research today lacks relevance to practice" (p.3). Surprisingly, almost thirty years after the Business Week criticism on how research is trapped in the Ivory Tower, these three words were repeatedly mentioned throughout our interviews with organizational decision-makers to refer to research regarding IT security in small-and medium sized enterprises (SME). Since these remarks during expert interviews cut deep into our self-concept as researchers with an aspiration to convey findings to both an academic and practitioner audience, we wondered: is our investigation of IT security investments in SME potentially still fuzzy, irrelevant, or pretentious, and do we insufficiently account for "the business and technological contexts in which IS phenomena transpire" (Benbasat & Zmud, 1999, p. 5)?

IT security can hardly be deemed irrelevant since persistent revelations of data breaches or ransomware attacks like NotPetya which resulted in estimated damages of more than 10 billion USD (Barrett, 2019; Greenberg, 2019) continuously demonstrate the practical relevance of this topic. Recognized as one of the Top 10 Global Risks according to the World Economic Forum (2019), issues like data fraud and cyberattacks have put a spotlight on the importance of securing IT systems in organizations and have thus far received ample attention from practice and theory (Angst et al., 2017; Coden et al., 2019; Straub & Welke, 1998; Wang et al., 2008). This attention also manifests itself in increasing IT security investments likely to exceed 124 billion USD in 2019 according to research company Gartner (Moore & Keen, 2019). However, the amount of investments vary dramatically according to the industrial sector and the enterprise size as evidenced by the lagging investment effort regarding IT security by SME (Zurich, 2017). Almost half (49 percent) of British SME, for example, plan to spend less than 1000 GBP on cyber security measures despite seeing themselves as ill-prepared for potential attacks (Kaspersky, 2017). This finding gives rise to the question, whether specifics of the business or technological context of SME remain overlooked.

Even though organizational IT security research represents an important subfield in IS, studies in this field are often based on samples from predominantly large enterprises (Angst et al., 2017; Hsu et al., 2015) or focus on specific industry sectors such as healthcare or finance (Kwon & Johnson, 2014; Wang et al., 2008; Yang & Lee, 2016). Consequently, this suggests that the majority of all companies might have been overlooked since SME make up over 90 percent of all enterprises globally (Eurostat, 2015; OECD, 1997). IS research and related disciplines have

acknowledged that SME are structurally fundamentally different from large enterprises since specific SME characteristics impact technology adoption or IS evaluation (Arendt, 2008; Ballantine et al., 1998; Cragg et al., 2011). Despite the relevance of SME, IS security research largely neglected the influence of SME characteristics.

Given the significant relevance of SME for both the economy and society, we advocate that organizational IT security research needs to take the particular characteristics of SME fully into account. We thus propose a framework that encompasses distinct SME characteristics identified in extant IS research and hypothesize how these function as constraints, ultimately influencing investment decisions regarding organizational IT security. In order to identify how internal SME-specific firm characteristics or external pressures and barriers affect their IT security investments, we interview decision-makers in SME. A total of 26 IT and business executives in SME participated in 25 semi-structured interviews. These interviews were subsequently analyzed to validate whether and how IT security investments are influenced by SME characteristics. Equipped with insights from this qualitative study, we discuss how extant research questions and methodologies along with explicit or implicit assumptions might be bounded by SME constraints. For example, assumptions like the existence of an IT department with security specialists (Spears & Barki, 2010; Sun et al., 2006) or the ability to collect and assess parameters necessary to estimate suggested decision models (Hu et al., 2007; Kumar et al., 2008; Yue & Cakanyildirim, 2007) do not represent the reality of most SME.

Consequently, our approach entails several important contributions for theory and practice. From a theoretical point of view, our results depict the apparent negligence of leading IS journals in representing the reality of SME in terms of organizational IT security. By highlighting the influence of SME-specific constraints in IT security investment decisions, we expose the necessity to expand, rethink, or constrain prevalent theories in organizational IT security research since extant findings are only generalizable to a limited degree. Additionally, our findings raise awareness for specific research gaps within the IT security field such as the tendency to neglect temporal and affective factors or to account for the level of procedural sophistication in SME. Practical implications should be considered by governments, larger companies with SME partners, and both user and provider organizations of IT security products and services. Governments and large companies should recognize the critical role of SME and find new ways to support them apart from currently imposed audits and indiscernible subsidy schemes. Providers can learn that top executives in SME differ in their decision-making process and often draw heavily on emotions and affects, while user organizations should embrace our results as

an indication to expand their timeframe and establish formalized and documented processes along with more strategic IS management practices.

8.2 Theoretical Background – Organizational IT Security Research

Building on previous research, we understand IT security in an organization as "the protection of information resources of a firm, where such protection could be through both technical means and by establishing adequate procedures, management controls and managing the behavior of people" (Dhillon & Torkzadeh, 2006, p. 299 referencing Dhillon (1997) and Baskerville (1989)). The subsequent literature review follows a representative coverage strategy (Cooper, 1988) and considers studies focusing on organizational aspects of IT security published within the Senior Scholars' Basket of Journals (SenS-8). We focused on the Sens-8 because it "recognizes topical, methodological, and geographical diversity" and could thus be seen as representative of the IS field (AIS, 2018; Lowry et al., 2013). Supplementary, we reviewed further databases to ensure the inclusion of additional relevant findings regarding organizational IT security in SME in other outlets.

8.2.1 Structured Literature Review – Method

Following Webster and Watson (2002) and Vom Brocke et al. (2009), we analyzed all papers published since the inception of the respective journals within the SenS-8, i.e., European Journal of Information Systems (EJIS), Information Systems Journal (ISJ), Information Systems Research (ISR), Journal of AIS (JAIS), Journal of Information Technology (JIT), Journal of MIS (JMIS), MIS Quarterly (MISQ), and Journal of Strategic Information Systems (JSIS). In line with the recommendations for a structured literature review, we defined the review scope and conceptualized the topic through the identification of all necessary keywords to capture as many studies as possible. This resulted in a keyword search term which can be extracted from Table 2 in the appendix along with the number of identified papers per journal and the exclusion criteria during all screening phases. The search term was used in two slightly varied versions according to the databases where the search was performed. We initially identified 320 papers via the keyword search. After an initial title screening, the abstract of the remaining 199 articles were analyzed to separate papers in an organizational context from mainly technical or legal studies and research focusing on Social Network Services (SNS), eCommerce, or end-user behavior. The resulting 105 articles were clustered in order to facilitate the full text screening and resulted in 10 clusters such as policy and compliance, outsourcing, risk analysis, conceptual

overviews and literature reviews. Due to the focus on organizational IT security from the perspective of decision-makers, only articles within the clusters security management and strategy (n=17), risk analysis (n=9), investment decisions (n=9), outsourcing and managed services (n=4), information sharing and vulnerability disclosure (n=4) along with 10 papers that could not be clustered due to their heterogeneity were further scrutinized using the propositions extracted from literature and expert interviews. The full text screening resulted in a further reduction of papers (n=28) on which forward and backward search was applied leading to the identification of one additional article within the Basket. The most relevant results of the SLR can be extracted from the Table 3 in the appendix and are discussed in the following section.

In addition to our SLR, we looked for further peer-reviewed articles outside the senior scholars' basket of eight by querying the databases ScienceDirect (title, abstract, keywords), ACM Digital Library (abstract), and the AIS Library (AISeL) (title, abstract, subject) using keywords such as "security" and "SME" or "startup". After a title, abstract, and full-text screening with subsequent backward and forward searches, we found six relevant additional articles that will be discussed below.

8.2.2 Structured Literature Review – Results

Given the focus on IT security investments in an SME context, we only briefly report the methodical approach and the theory or model the final studies are based on. In the following, we analyze the structure of their sample and how these articles focus and consider IT security investment and the SME context in general de facto.

Since the inclusion of SME was of central interest for his structured literature review, studies that actually report their sample or study context could give first insight into whether and how the SME context was accounted for. Almost half of the identified articles do not base their findings on a specific sample, but rather take a conceptual approach (Baskerville, 1991; Wolff, 2016), use mathematical modelling (Cavusoglu et al., 2008; Chen et al., 2011; Gal-Or & Ghose, 2005; Hui et al., 2012; Kumar et al., 2008; Lee et al., 2013; Sen & Borle, 2015; Yue & Cakanyildirim, 2007; Zhao et al., 2013), or review extant literature (Dhillon & Backhouse, 2001; Siponen, 2005). Only a total of fourteen papers followed either a qualitative approach (Dhillon & Torkzadeh, 2006; Hsu, 2009; Hu et al., 2007; Straub & Welke, 1998), conducted a quantitative/empirical study (Angst et al., 2017; Gordon et al., 2010; Herath & Herath, 2008; Kwon & Johnson, 2014; Lee & Larsen, 2009; Wang et al., 2008), or pursued a combined, mixed-method approach (Hsu et al., 2012; Spears & Barki, 2010; Straub, 1990; Wang et al.,

2013). Out of these, only one study exhibits a distinct SME focus through their sample (Lee & Larsen, 2009) whereas two other study samples explicitly contain SME (Angst et al., 2017; Dhillon & Torkzadeh, 2006) and several others only potentially include SME since they omit detailed or clear sample characteristics (Gordon et al., 2010; Kwon & Johnson, 2014; Spears & Barki, 2010; Straub, 1990).

With the exception of Angst and colleagues (2017) who establish hospital size to exert influence on IT security investments and the implementation of security measures, only Lee and Larsen's (2009) study manifests a clear focus on SME and argues for the influence of SME characteristics regarding investment decisions in organizational IT security. Among the other papers that do consider IT security investment as an antecedent or the outcome of their studies, only the study of Gal-Or and Ghose (2005) – who investigate the competitive implications of sharing security information, in terms of successful and unsuccessful attempts at security breaches, and investments in security technologies – displays some consideration of SME characteristics since they consider firm size. However, comparable to studies of Dhillon and Torkzadeh (2006), Gordon and colleagues (2010), Kwon and Johnson (2014), or Straub (1990), they do not discuss and elaborate how specific firm characteristics might affect investments, but draw on the notion that firm size is intertwined with the number of firms in the industry: A higher degree of concentration of firms, i.e. a decreasing number of firms, leads to an increase of the marginal benefit from technology investment and information sharing (Gal-Or & Ghose, 2005).

Lee and Larsen (2009) on the other hand study the decision of SME executives to adopt anti-malware software via the application of the Protection Motivation Theory (PMT) (Rogers, 1983). Their approach is also motivated by the lack of studies focusing on small and medium-sized businesses and the necessity to account for the "interplay among organizational properties, human agents and technology" (p.178). Drawing on Thong's (1999) model of information systems adoption in small businesses, they extend PMT with social influence and situation-specific behavioral control variables (vendor support, IT budget, firm size). The latter three variables were derived from previous interviews and selective considerations of extant IS adoption research (e.g., Forman, 2005; Iacovou et al., 1995; Thong, 1999). Rather counterintuitively, Lee and Larsen's (2009) study found no evidence that firm size significantly influences adoption intention and actual adoption but showed that IT budget and vendor support played a key role in purchasing anti-malware software. However, their findings still suggest that specific SME characteristics exert an influence on investment decisions – but only cover a total of three

of these characteristics despite numerous SME studies in an IS context suggesting other important characteristics (Beck & Demirguc-Kunt, 2006; Caldeira & Ward, 2003; Chen et al., 2007; Dholakia & Kshetri, 2004). Additionally, their SME definition covers firms with fewer than 500 employees in line with previous researchers and the US Small Business Administration (Riemenschneider et al., 2003; United States Business Administration, 2018). This definition is in stark contrast with the official terminology of the European Union and many other countries with limits at 200 or 250 employees and their inclusion of further factors such as annual turnover (OECD, 2005).

Our additional search for SME IT security publications outside the basket of eight underlined this necessity for a common understanding of SME due to differing definitions (e.g., Keller et al., 2005) or the entire omission thereof (e.g., Barton et al., 2016). Despite the stated focus on SME and IT security, half of the identified articles were purely conceptual or included mathematical modelling (Fielder et al., 2016; Mayadunne & Park, 2016; Ng & Feng, 2006) whereas the other half was split into one qualitative empirical study focusing on current trends (Keller et al., 2005) and two survey-based studies (Barton et al., 2016; Yildirim, et al., 2011). Only the studies by Barton et al. (2016), Ng et al. (2006), Yildirim et al. (2011) aim at dissecting influencing factors in IT security studies, drawing partly on Straub (1990), Straub and Welke (1998), or Lee and Larsen (2009), i.e., on both selected organizational and behavioral factors.

Drawing on the findings of our structured literature review, we argue for the necessity to first define the term “SME” and to examine previously identified SME characteristics in further detail. After defining and demonstrating the global relevance of SME, we build on previous SME research (Caldeira & Ward, 2003; Cragg et al., 2011) to build a framework and to derive propositions on how these identified characteristics affect organizational IT security investments in SME.

8.3 SME in IS Research – Definition, Relevance, and Framework

8.3.1 Definition and Relevance of SME

The term “Small and Medium-sized Enterprise” (SME) or SMB for small and medium-sized businesses commonly refers to the biggest business sector in both the industrialized world and developing countries (Ballantine et al., 1998). Commonly, SME are defined as non-subsidiary, independent organizations which employ less than a certain number of people which varies according to national statistical systems (OECD, 2005). While there is no universally accepted

definition of SME on a global and also often on a national level, most North-American institutions set the upper limit at 500 employees for most organizations (manufacturing and non-exporting services firms, exporting services firms, and farms) with differing annual firm revenue limits ranging from 250,000 USD to 25 million USD (USITC 2010). Other countries define SME with a maximum number of employees of 100 (e.g., Kenia, Nigeria) or 200 (e.g., South Africa, Singapore). Chinese definitions are rather complex and based on the SME Promotion Law of China which differentiates additionally between industry sectors and headcounts up to 1000 employees (OECD, 2016). One of the most frequent upper limits however is the 250 employee cutoff proposed by the European Commission (2003). Along with classification criteria for turnover and balance sheet total, the European definition of SME proposes the following company categories: very small or micro-enterprises (less than 10 employees, less than 2 million EUR turnover and balance sheet total); small enterprises (less than 50 employees, less than 10 million EUR turnover and balance sheet total); medium-sized enterprises (less than 250 employees, less than 50 million EUR turnover and 43 million EUR balance sheet total).

According to the World Trade Organization, micro-enterprises dominate the business landscape in all countries since they account for 70 to 90 percent of all firms globally (WTO, 2016). In the non-financial sector, SME even represent 99.7 percent of all firms in the OECD area while accounting for 60 percent of the respective total national employment (OECD, 2017). The percentage of total employment and job creation along with the SME share of a country's GDP and their contribution to innovations, have earned SME the reputation to be the "backbone" or "bedrock" of their respective country's economy (Dutta & Evrard, 1999; Verhees & Meulenberg, 2004). Regarding the important role of SME, it is unsurprising that research has been dedicated to understand how SME might differ on a structural level from large enterprises and why SME are seemingly more affected by the so-called "digital divide" (Boyes & Irani, 2003; Cragg et al., 2011; Wielicki & Arendt, 2010). This digital divide refers to the notion that SME lag behind large enterprises when it comes to harnessing technological innovation and to be a beneficiary thereof in the age of digital transformation. Since adoption of IS technologies is a cornerstone, much research attention has been dedicated to potential influential factors that are unique in the SME context. We thus set out to provide an overview over SME characteristics that have been identified in prior IS research as potential constraints and barriers SME are commonly confronted with.

8.3.2 Extant IS Research regarding SME Characteristics and Propositions for IT Security Investments

Drawing on the typology of Paré et al. (2015) and the process outlined by Webster and Watson (2002), we performed a theoretical review to develop a conceptual framework. The search process was initiated with a rather broad research question and the respective keywords ("Which challenges, barriers, characteristics are associated with SME in IS literature?"). We queried the AIS Library and Web of Science focusing on highly cited publications such as Thong (1999) or Caldeira and Ward (2003) and relied on an iterative approach via forward and backward search pursuing a representative coverage and neutral representation while focusing on integrating research outcomes according to Cooper (1988). Consequently, we identified several external barriers and pressures associated with characteristics of the SME's (external) micro and macro environment as well as characteristics internal to the focal firm which could act as constraints regarding IT security investments. The resulting framework depicted in Figure 1 represents a condensation of extant models and examinations performed by various researchers and practitioners (Boyes & Irani, 2003; Caldeira & Ward, 2003; Chang & Wang, 2011; Cragg et al., 2011; Dojkovski et al., 2007; OECD, 2017):

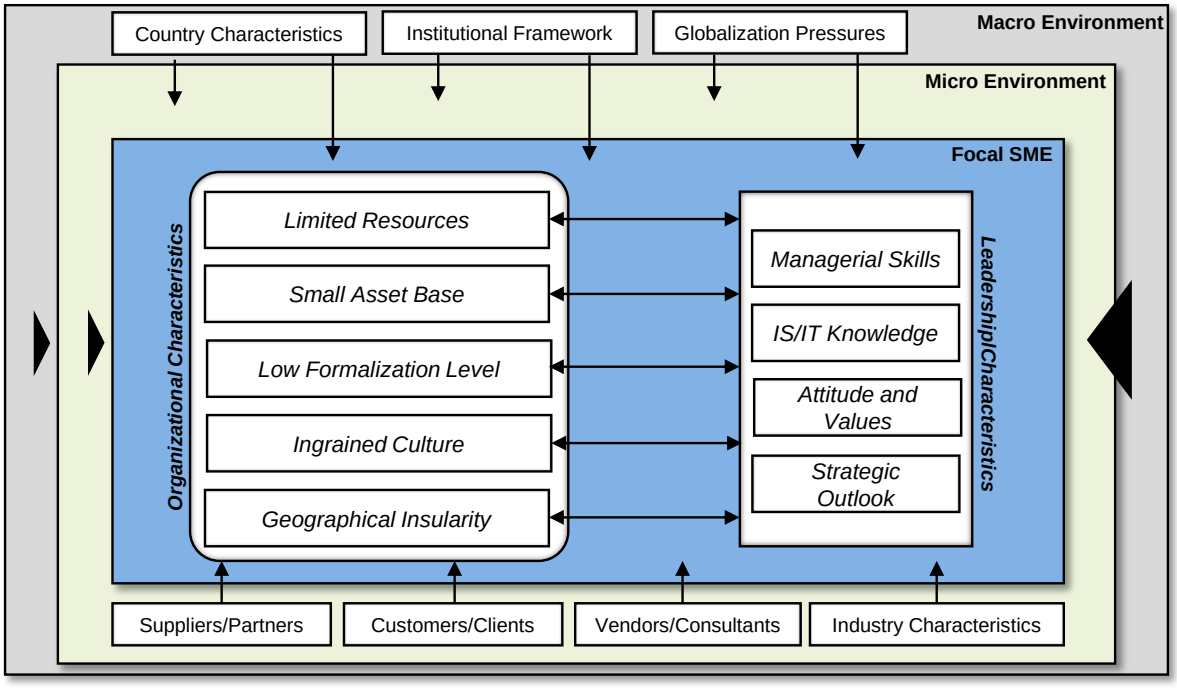

Figure 14. Conceptual Framework of SME Constraints

The framework comprises three layers, namely the Macro Environment (grey box), the Micro Environment (green box), and the Focal SME (blue box) and is consistent with other organizational studies investigating the influence of internal and external characteristics in information

technology (Melville et al., 2004; Weishäupl et al., 2015). The outer layer, **Macro Environment**, comprises country characteristics like national culture, the institutional framework in terms of legal regulations, and general globalization pressures which are not necessarily specific to the SME context, but often affect smaller companies to a greater extent compared to large enterprises. Exemplary are legal changes where compliance is potentially more difficult for SME due to a lack of available legal staff and expertise or hindered access to foreign markets due to a dependence on trading partners and lower trading power (Chen et al., 2007; Piscitello & Sgobbi, 2004).

The middle layer, **Micro Environment**, is the direct periphery of the SME, i.e., suppliers/partners, customers/clients, vendors/consultants and general industry-specific characteristics which affect the enterprise through competitive pressure (Melville et al., 2004; Stockdale & Standing, 2006; Teo et al., 2004). For instance, SME are particularly pressured due to their position at the end of the value and supply chain, as evidenced by so-called auditing chains and are typically regarded as price-takers (Casterella et al., 2004). These external characteristics of the SME micro and macro environment are not of central interest in this study and will thus not be investigated further but are mentioned and depicted for the sake of completeness.

The following qualitative study focuses on organizational and individual constraints of the focal SME depicted in the blue inner box "**Focal SME**" in Figure 1. This layer consists of distinct organizational characteristics and leadership characteristics which are interrelated and influenced by the respective micro and macro environment of the focal SME (Chell et al., 1991; MacGregor & Vrazalic, 2005). Previous SME research finds that leadership characteristics of the owner-manager or managing director and organizational characteristics strongly influence how the focal SME operates and how (investment) decisions are made within the enterprise. In the following, we will first elaborate how typical organizational characteristics of SME potentially influence IT security investments before we elaborate on the interplay of IT security investments and SME leadership characteristics.

The prominence of Organizational Characteristics can often be directly linked to the number of employees or the categorization of an SME into a micro, small, or medium-sized enterprise. In an IS context, studies suggest that certain characteristics of SME also apply to enterprises or (non-profit) organizations that employ a very small number of IT professionals (Muehe & Drechsler, 2017). This lack of skilled workforce can be easily translated into of the most common characteristics of small business, namely limited resources.

Limited Resources commonly refer to a shortage of financial assets and knowhow or expertise (Boyes & Irani, 2003; Thong, 2001). The latter can be a result of high labor costs and a lack of human resources or skilled workforce that affects SME in particular (Buckley, 1997; MacGregor, 2003). Since SME simply cannot "afford" several IT experts, they either have to rely on generalists or "involuntary" IT managers (Bradshaw et al., 2013; Cragg et al., 2013). Outsourcing certain areas in IS to IT consultants could thus be a beneficial reaction but is constrained by limited budget which is among the most prominent features in SME. Previous research states that business decisions like investments or IS adoptions are often strongly affected by financial and skill constraints (Chen et al., 2007), hence we posit:

> ***Proposition P1***. *Limited resources will negatively influence IT security investments in an SME context.*

The Small Asset Base represents another and one of the most frequently cited constraints for SME. This aspect comprises both the difficulties of SME to access external financial resources (Carbo-Valverde et al., 2007; Riemenschneider et al., 2003) and general cash flow difficulties (Welsh & White, 1981). Additionally, SME capital is often bound to the owners, thus potentially leading to a restricted capacity for strategic, long-term economic risk and investments (Howorth, 2001) which leads to the following proposition:

> ***Proposition P2***. *A small asset base will negatively influence IT security investments in an SME context.*

Low Formalization Level in SME is closely linked to the above-mentioned constraints. It describes the existence of dual or even multiple role-identities ascribed to one individual person, e.g., IT functions and general management tasks are performed by one person due to a shortage of skilled personnel or time. Additionally, CEOs often execute administrative tasks and have to make business decisions while drawing on ad hoc, non-formalized, undocumented management practices resulting in a rather low procedural sophistication and highly centralized structures (Chell et al., 1991; Mintzberg, 1989). Since documentation processes and information flows are highly important to determine which technology or which security measure should be adopted, we assume the following:

> ***Proposition P3***. *A low formalization level will negatively influence IT security investments in an SME context.*

Another organizational characteristic that relates to both internal processes and the micro-environment is the unique organizational culture or ingrained culture in SME that is shaped by flat

hierarchies, direct and short communication channels with organizational decision-makers, and the distinct role of trust in business relationships (Cragg et al., 2011). An overreliance on strong business ties that are based on long-term trust relationships can however lead to or aggravate a certain preservation or backwardness in terms of business culture (Caldeira & Ward, 2003). This in turn largely constrains an open culture within the company and the relationship towards the greater micro-environment which prevents access to other or new information sources and business partners (Agell, 2004; Bennett & Robson, 2004). However, the ever-growing complexity and novelty of both IT security threats and solutions requires to rethink existing business processes, draw on new information sources, and to consider new business relationships with unknown solution providers. The more ingrained and inflexible the culture in an SME, the more unlikely IT security investments become. Hence, we posit:

> ***Proposition P4***. *Ingrained culture will negatively influence IT security investments in an SME context.*

Similarly, (geographical) Insularity of SME as stated by Bharati and Chaudhury (2009) can constrain IT/IS adoption and investment decisions in general. They explain that SME are often limited in their interaction with their environment due to their location and generally maintain the most important business relationships with suppliers, partners, and customers in a limited geographical area. This lock-in is further aggravated by an overreliance of the aforementioned strong ties within the closest community. Since growing complexity in information systems and the emergence of new IT security attack patterns make objective judgments particularly challenging, organizational responses to adopt new technology or invest in adequate countermeasures are often influenced by subjective or social norms (Ajzen, 1991; Angst et al., 2017; Fishbein & Ajzen, 1975). The more insular an SME is, the more pronounced is the negative effect on IT security investments:

> ***Proposition P5***. *Geographical insularity will negatively influence IT security investments in an SME context.*

Leadership Characteristics are especially relevant in an SME context due to the influential role of owner-managers since they are often the prime and sole decision-maker in every operational and strategic business aspect all while being almost exclusively responsible for the survival of the enterprise (Birley, 1982; Thong, 1999; Thong & Yap, 1995). Researchers have thus pointed out that leadership competences like managerial skills and IS/IT knowledge, their general attitude and values, as well as their strategic orientation strongly influence if and how investments in IS/IT are made (MacGregor & Vrazalic, 2005).

The need for pronounced Managerial Skills is especially relevant in an SME context as decision-makers often have to "juggle" a multitude of role identities since owner-managers often simultaneously function as chief executive officer (CEO), managing or IT director. Appropriate managerial skills are important because most IT investments entail change and project management (Cragg et al., 2011) along with strategic and operational alignment between business and technology to ensure the focal firm's successful and beneficial exploitation of IT (Feeny & Willcocks, 1998). Since managerial skills are a prerequisite for technology evaluation and generally affect the overall success of technology adoption (Thong, 1999), we also assume that they will play an important role in IT security investments:

> ***Proposition P6****. Managerial skills will influence IT security investments strongly in an SME context.*

Previous IS research has additionally identified that owner-managers who are more knowledgeable or more inclined towards technology and information systems appear to be quicker at adopting and adapting to technological innovations despite the growing complexity of the IS field (Caldeira & Ward, 2003; Thong, 1999; Thong & Yap, 1995). Drawing on Caldeira and Ward's (2003) findings, a follow-up study on organizational IS competences in SME by Cragg and colleagues (2011) have argued for the link between individual level technical skills and technical IS/IT skills. A basic level of individual IS/IT Knowledge and skills is thus a prerequisite for organizational IS/IT processes such as purchasing decisions, hence we assume that a similar relationship will be evident regarding IT security investments:

> ***Proposition P7****. IS/IT (security) knowledge of the decision-maker/owner-manager will positively affect IT security investments in an SME context.*

Since the role of the owner in small businesses is pivotal, various researchers have constituted that individual characteristics such as the disposition towards technology or the personal risk attitude affect decision-making processes. Attitude in particular has been extensively demonstrated to influence the intention to accept and use new IS/IT (e.g., Ajzen, 1991; Dwivedi et al., 2017; Fishbein & Ajzen, 1975; Riemenschneider et al., 2003). Since extant organizational IT security research confirms that managers' concern over systems security vary according to their individual characteristics and values (Goodhue & Straub, 1991; Hsu et al., 2012), we believe the same mechanism to hold true in an SME context – possibly even to a heightened degree given the pivotal role of decision-makers, assuming that:

> ***Proposition P8****. The personal attitude and values of the decision-maker/owner-manager will heavily influence IT security investments in SME.*

Finally, entrepreneurial or adoption studies have highlighted the crucial role of Strategic Outlook, i.e., long-term planning and thinking when introducing new concepts or technologies (Bassellier et al., 2001; Drechsler & Weißschädel, 2018; Feeny & Willcocks, 1998). This strategic outlook is however largely constrained in smaller enterprises since "strategy and planning were typically short term in an SME" (Cragg et al., 2011, p. 353). We thus expect that strategic outlook and specifically long-term planning will positively influence investment decisions in IT security, whereas an operational perspective and short-term planning will negatively affect investment decisions. Due to the pivotal role of decision-makers in SME, we assume that the time horizon will play a pronounced role in an SME context:

> ***Proposition P9****. The strategic outlook of the decision-maker/owner-manager will influence IT security investments in an SME context.*

8.4 Qualitative Study

8.4.1 Method and Research Design

We employed a qualitative study to assess our propositions within an SME context. Following Kaplan and Maxwell (1994), we argue that it is important to understand perceived boundaries and constraints from the point of view of participants in the particular social and institutional context – in our case relevant decision-makers in SME of both user and provider firms. Whereas the dominant stream of IT security literature employs quantitative research methods, we argue that certain covert assumptions or preconceptions might be irrelevant or incongruous for the SME context. In order to challenge these assumptions, we advocate for the necessity to "see the world through the eyes of the actors doing the acting" (Greener, 2008, p. 17), i.e., employing a qualitative approach using interviews with experts within that particular context. As our approach is based on a conceptual framework, thus relying on stated knowledge, yet still embraces the skepticism innate to interpretivist approaches, an epistemological post-positivist stance allows for a more comprehensive explanation of the context of the studied phenomenon (Fischer, 1998). Our approach sets out to broaden the current state of IS research in organizational IT security in SME by questioning experts – both from the perspective of IT staff and executives from user and provider firms.

Our design and reporting phase adheres to guiding principles offered by Sarker et al. (2013). Following these guidelines, we prepared an interview protocol resulting in semi-structured interviews with key informants in different organizations. In order to overcome typical pitfalls of semi-structured interviews like the artificiality of the interview or lack of trust, we followed

Goffman's recommendation of seeing the qualitative interview as a drama with a stage, props, actors, an audience, a script, and the actual performance (Goffman, 1959). Especially, first impressions are seen as crucial for the success of the interview. Hence, email and telephone contact was used prior to the interview and the actor, i.e., the interviewer, showed empathy and understanding to decrease the chances of the interview going awry (Hermanns, 2004). The initial script itself included several strategies regarding the type of questions asked, e.g., meaning questions to evoke previous experiences with IT security measures and decisions, process questions to identify a longitudinal change regarding IT security, or descriptive questions aimed at identifying underlying beliefs and practices of the investigated social group (Morse, 1994). Additionally, provocative, or ideal questions were posed in order to elicit perceived constraints (e.g., "In your opinion, what would be necessary to achieve an ideal status quo of organizational IT security in your company and in other SME?"). Due to the semi-structured approach, initial questions were subject to change and adapted to the respective interview partners and their position or knowledge throughout the interviewing process. Exemplary questions of our initial interview guide can be found in Table 4 in the appendix. The guide covered the following five broad topics and included exemplary questions as indicated in brackets: (1) company profile (e.g., "Please provide a short description of your company and role."), (2) IT security status quo (e.g., "How would you rate the IT security awareness in your company?"), (3) processes and assessments (e.g., "How do you decide upon IT security investments?"), (4) stakeholder perspective (e.g., "Which kind of external support do you consider regarding IT security investments and implementation?"), and (5) need for action (e.g., "What need for action do you see in the area of IT security, especially for SME?").

8.4.2 Sample

From November 2017 until February 2018, CEOs or owners and IT executives of SME in a Western European country were identified via an online social business network and the local Chamber of Industry and Commerce. The invited interview partners were chosen in a key informant approach from user firms (Coden et al., 2016), user and provider firms (UPF), and later on also from provider firms (PF). This distinction is based mostly on the product or services portfolio of the respective firm employing our interview partners. While UF are purely clients of IT security services and products, PF are mainly suppliers of such goods, and UPF introduced security services or products recently to diversify their established IT portfolio.

In order to avoid an elite bias, both IT staff and executives were invited (Miles & Huberman, 1994). Due to the semi-structured approach and additionally derived insights from interview

partners, executives and staff from IT security providers were additionally invited to participate. While most interviews were held face-to-face because of the rather intricate and sensitive nature of the topic, a total of seven interviews were performed via phone calls due to geographical distance. Seven interview partners identified themselves with a pure IT role, while two held a hybrid position and 13 were top executives and managing directors (MD). Another four interview partners were either responsible for sales or consultancy. Only one of the interview partners was female. The majority of participants (60 percent) are active in the service sector while 24 percent of the sample organizations provide a mixture of services and manufactured goods, eight percent each are either focusing on production or trade. The self-stated role(s) of the interview partners and their respective experience (Job Exp.) in their role as well as their companies' classification of economic activity according to the ISIC classification (United Nations, 2008), the specific sector and size are depicted in Table 13.

ID	Position	Job Exp.	Other Responsibilities	ISIC	Firm's Sector	Size	Interview Method
Group: User Firm: Key informants of firms that are solely users of IT security products and services							
UF-01	Director IT	19 years	-	C	Chemical Manufacturing	m	Face-to-face
UF-02	MD	10 years	IT Administrator	M	Marketing Services	vs	Face-to-face
UF-03	CIO	40 years	-	P	Educational Services	m	Face-to-face
UF-04	MD	22 years	Owner	C	Mechanical Engineering	m	Face-to-face
	Director IT	20 years	-				
UF-05	MD	20 years	IT Administrator	M	Legal Services	s	Face-to-face
UF-06	MD	12 years	IT Administrator	F	Building Reconstruction	s	Face-to-face
UF-07	MD	5 years	IT Administrator	M	Marketing Services	vs	Telephone
UF-08	Director IT	7 years	-	G	Retail	m	Face-to-face
UF-09	MD	10 years	IT Administrator	N	HR Services	s	Face-to-face
UF-10	MD	4 years	Sales Manager	M	Marketing Services	m	Telephone
UF-11	Director IT	18 years	-	G	Wholesale	s	Telephone
UF-12	MD	10 years	Sales Manager	M	Marketing Services	s	Face-to-face
UF-13	MD	8 years	Consultant	M	Consultancy	s	Face-to-face
UF-14	MD	4 years	Consultant	M	Consultancy	vs	Face-to-face
UF-15	Director IT	5 years	Project Manager	P	Educational Services	s	Face-to-face
UF-16	Consultant	6 years	IT Administrator	J	IT Project Management	s	Face-to-face
UF-17	MD	2 years	IT Administrator	M	Legal Services	vs	Face-to-face
UF-18	CIO	20 years	-	N	Relocation Services	s	Face-to-face
Group: User and Provider Firm (UPF): Key informants of firms that are both users and providers of IT security products and services							
UPF-01	MD	10 years	CIO	J	Publishing and IT Services	s	Face-to-face
UPF-02	Director IT	20 years	-	J	Publishing and IT Services	m	Face-to-face
Group: Provider Firm (PF): Key informants of firms that are providers of IT security products and services							
PF-01	Sales	5 years	Consultant	J,M	IT Services	s	Face-to-face
PF-02	MD	21 years	-	J,M	IT Services	s	Telephone
PF-03	Consultant	19 years	-	J,M	IT Services	m	Telephone
PF-04	Sales	2 years	Consultant	J,M	IT Services	m	Telephone
PF-05	MD	20 years	-	J,M	IT Services	s	Telephone
ISIC Codes (United Nations 2008): C= Manufacturing; F= Construction; G= Wholesale and Retail Trade; J= Information and Communication; M= Professional, Scientific and Technical Activities; N= Administrative and Support Service Activities; P= Education; **Firm Size**: vs= very small (1-9 employees); s= small (10-49 employees); m= medium (50-249 employees)							

Table 13. Participant Overview

All interviews (length average of 72 minutes) were recorded and transcribed by mutual agreement and enriched by field notes of the researchers. All interviewees were guaranteed anonymity and offered an executive report of the results. No additional interviews were scheduled after the 25th interview because further contribution through additional qualitative data to a concept or a relationship between concepts was deemed unlikely after the fifth provider was interviewed (i.e., theoretical saturation was assumed). This quantity of interviews is comparable to other organizational IS (security) publications (Marshall et al., 2013; Sonnenschein et al., 2017).

8.4.3 Data Analysis Technique

In line with the philosophical stance and the developed conceptual framework, the transcripts were analyzed using an iterative multi-level coding process similar to extant IS (e.g., Albrechtsen, 2007). Coding cycles were used to answer our research questions as displayed in Figure 15 following the suggested techniques of Miles and colleagues (2013).

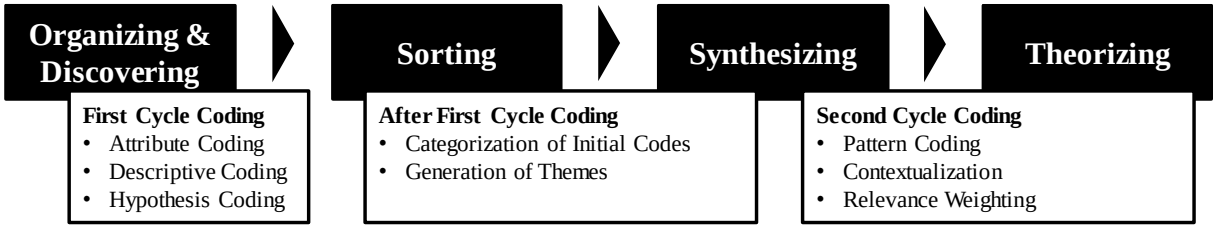

Figure 15. Analysis Technique

After an initial familiarization with the transcripts and simultaneous memo-ing, the First Cycle consisted of attribute, descriptive, and hypotheses coding using MAXQDA software to facilitate the analysis process (Bazeley, 2003). Attribute coding (or context coding) was used to identify essential information about the data at hand and demographic characteristics – for example, age, gender, experience, position, time frame – resulting in an overview of the sample (see Table 1) and in a potential attribute base used to expose interrelationships or themes in a later coding stage (Bogdan & Biklen, 2007). Furthermore, descriptive coding was employed to summarize topics resulting in a general categorized code inventory which provided a basis for additional, more focused analysis and interpretation (Wolcott, 1994). This coding technique was primarily used to possibly extend the initially developed conceptual framework by disregarding the previously identified constraint dimensions (i.e., limited resources, small asset base, low formalization level, ingrained culture, geographical insularity, and leadership characteristics). Descriptive coding was mainly employed to identify further potential constraints and their

manifestations. As recommended by Saldaña (2009), hypothesis coding was performed subsequently to account for the initially conceptualized constraints and to screen the scripts for verbatim and in spirit mentions (Auerbach & Silverstein, 2003). For example, statements regarding the resource situation were further analyzed and broken down into themes, e.g., specific resource aspects like budget or time. The first coding cycle thus helped to gain a general and broad overview by identifying relevant themes regarding IT security investments. Subsequently, resulting initial codes were once again categorized into themes, i.e., the distinct manifestations of the aforementioned constraint dimensions during the sorting and synthesizing steps. These themes were further analyzed during the Second Cycle through pattern coding, contextualization, and relevance weighting which served as a lens to examine further patterns or explanations for the subsequent theorizing stage (Miles & Huberman, 1994).

Several practices were employed throughout the coding and analysis process in order to achieve rigor and trustworthiness: The data analysis was led by clear propositions and prior theorizing served as the base of the conceptual framework and was used as input to our research design. In terms of the selected interviewees, a broad range of highly involved individuals across several industries enable extensive comparisons and potentially yield more general research results (Benbasat et al., 1987). Furthermore, the data collection was supported by data triangulation by including both IT and business executives from user and providers of IT security measures while field notes and a multi-researcher triangulation was employed during data analysis. Other tactics, as proposed by Miles and colleagues (2013), included weighting the evidence to identify the most trustable data and to pay attention to "unpatterns" by checking for outliers, extreme cases, and negative evidence. Furthermore, the following presentation of findings including direct quotes brings "the voice of participants in the study" (Creswell, 1998, p. 70), while contributing to transparency and accountability.

8.4.4 Results

The propositions stated in 3.2. and the visualized influence of SME characteristics (Figure 1) were supported to differing degrees as interviewees perceived certain characteristics as more relevant or severe in their specific environment. While manifestations of limited resources and attitude along with strategic outlook were most prevalent and deemed relevant unanimously, insularity or small asset base received differing support. The latter two constraint manifestations were mentioned more often by managing directors of user firms. In contrast, manifestations of low formalization level and insularity (excluding geographical insularity) received more attention and higher relevance ratings by IT executives of user firms and interviewees

from provider firms. In the following, we provide more detailed findings on how the previously identified SME constraints manifest themselves in an IT security context.

Organizational Characteristics

Limited Resources were among the constraints most often mentioned by all interviewees across firms and positions. The manifestations of these constraints in an organizational IT security context refer particularly to limited budget, time, and workforce which are all highly interrelated, yet influence IT security investments distinctively as illustrated in the following.

Limited financial resources were mentioned most frequently by managing directors and very often by IT staff and interviewees from provider firms in line with a multitude of SME studies. Especially, owners and managers of smaller businesses see IT security investments as a strong cut into their finances. Also, when asked how they see their own company's organizational IT security status compared to larger companies, managing directors often attribute a better status in large companies to the available financial resources. The influence of limited budget is evidenced by the following statement:

> *"I mean, I did try to inform myself about it and the smallest server we'd need costs 4000€! Well yes, 4000€ is a lot of money!" – UF-02, Managing director*

Limited time was among the most frequently stated constraints in our sample across roles. Especially, managing directors pointed out that managing IT security requires a lot of time for them personally as well as across the entire organization. Notably, statements regarding time often included the phrase "I have to take/make time". Dealing with IT security and decisions regarding the investment in IT security measures are generally seen as additional tasks that can be performed only by cutting time expenditure on other important organizational duties. These statements are also intertwined with manifestations of low formalization levels regarding multiple roles and responsibilities within one position. This perspective is also shared by interviewees from provider companies and IT executives in user companies:

> *"[IT security as a topic] is something you have to research a lot to learn the ropes, to familiarize yourself. If we actually think about implementing a solution that is recommended, it can become too time-consuming for us. In some cases, it might be better to attend trainings but that is something only a full-time IT administrator could do […]." - UF-16, Consultant in a user firm who is also responsible for IT administration*

Limited knowhow was mentioned frequently by all interviewees and is strongly intertwined with the aforementioned resource constraints. This constraint manifests itself in two distinct

ways: [A] SME do not employ any specialized IT personnel with enough knowhow regarding IT security or [B] the IT personnel is already fully stretched and cannot be involved in IT security projects. The latter option was brought forward especially by interviewees with an IT background. Managing directors often mentioned a general shortage of skilled IT workers and lacking knowhow intertwined with insufficient awareness regarding IT security in SME altogether:

> *"Well, I would say that SME do not care enough or not at all to actually deal with IT security issues, because – I think – there are no employees with enough knowhow regarding IT", UF-09, Managing director*

Small Asset Base was one of the less prominent constraints mentioned. However, we could still find evidence that a small or irregular revenue stream affects IT security investments:

> *"And especially small or medium-sized startups do not have a steady revenue, so there is no money left for IT security spending." – UF-15, CIO*

Even though the initial literature review on SME constraints stresses the difficulty to obtain external financial support, a few interviewees actually expressed that funding and subsidies are readily available whereas some managing directors pointed out the difficulty to obtain certain grants or the ignorance of their existence altogether. No interviewee mentioned that they ever had to rely on external financial support for any IT security investments, hence any distinct influence of this constraint could not be upheld sufficiently. Limited backing for this constraint can be evidenced through the following statement:

> *"There are a couple of good loans available and one should debate whether it is truly necessary to finance an investment always via one's own cash flow or if it is possible to get some [external] support. […]. Certainly, there are very attractive schemes – it's only that no one knows about them." – UF-12, CIO*

As for owner capital, interviewees who were the actual owners mentioned sporadically that any decision regarding IT security investment required them to draw on their personal funds. IT directors and providers indirectly regarded this constraint manifestation as a possible hindrance for further investments arguing that the actual "value" or return on investment has to be explicated in more detail if owner have to spend their own money on something as intangible as IT security measures.

> *"This actually means that I don't have the financial means, if I don't reach deeper into my own pockets and say: 'I'll pay someone ten to twenty thousand Euro in a lump sum'. I think this is true for the majority of companies [SME]" – UF-07, Managing director*

The ***Low Formalization Level,*** or a lack of infrastructure, strategic planning, or processes are a common theme when discussing SME constraints in general. Against the backdrop of IT security, three themes emerged frequently, namely budget planning (or the lack thereof), multiple roles or responsibilities within one position, and undocumented processes which negatively impact IT security investment.

When asked about possible hindrances to IT security investment, IT staff and providers mentioned a lack of budget planning as being a decisive factor. Likewise, some managing directors admitted that they do not have a structured budget planning process in general or for IT (security) spending in particular.

> *"It [budget planning] does exist of course but it is a glorious exception in my professional experience! In most companies, it'll go according to the guiding theme 'when we need it, we get it'" – PF-05, Managing director*

As mentioned earlier, limited time can be both seen as consequence and reason for the existence of multiple roles and responsibilities within one position. This understaffing is a common feature in SME and their management of information systems as illustrated by West (1975) who states that, "almost without exception, the small company is grossly understaffed, often being a one-man operation." As already illustrated in our sample table (Table 1), many managing directors are additionally responsible for IT and IT security issues, while some IT staff also have to cope with several roles and responsibilities other than usual administrative tasks, e.g., setting up new devices for colleagues or new programs. In this regard, both managing directors and IT staff mentioned the plethora of tasks that are of higher priority resulting in IT security being a topic that is often neglected and followed up with the sole goal of not causing too much damage:

> *"Like I mentioned earlier, the only thing you can try to do is to avoid acting grossly negligent. My problem is honestly that, given the many things I have to do every day, and all the issues that keep on bombarding me… well, I would like to act rather than react all the time. But that is truly difficult." – UPF-01, Managing director*

The last manifestations of a low formalization level are non-existent, undefined or undocumented (organizational and technological) processes paired with "ad hoc" decision-making. This was most commonly expressed and deemed highly relevant by provider companies and experienced IT personnel. Especially, interviewees of provider companies saw an additional problem in unawareness of top managers in SME for the necessity of documented organizational and technological processes – which will be further discussed in the following section on

leadership characteristics. Documentation in particular is not consistently carried out in smaller companies. This complicates the service of providers who need to invest considerable time and effort into comprehending the extant IT architecture before actual measures can be implemented. In this regard, younger companies or startups seem to have a strategic advantage compared to incumbent, more traditional SME since they do not have to take legacy IT infrastructure into account and can thus set up a lean – often cloud-based and pre-secured – infrastructure from day 1 on. In incumbent SME, especially IT directors in medium-sized companies pointed out that they had to assess all existing processes and structures for the first time within their company – when they joined the firm or the enforcement date of the EU General Data Protection Regulation (GDPR) approached – which confirms the assumption of low procedural sophistication in SME. Interviewees from provider companies that "enter" user companies externally, view this low sophistication of documentation and processes especially dramatic:

> *"In many cases, you will find organically grown structures that are clear to no one. Someone has put a storage here, someone has done something else there. Sometimes companies have double storage, but they don't even know about the existence of both!" – PF-01, Business development executive*

Ingrained Culture, manifested via trust-based relationships, deeply-rooted organizational traditions and company hierarchy, was a constraint often emphasized by providers. Both interviewees from user and provider companies pointed out that trust was extremely important both between the IT director and the managing director as well as between the final decision-maker within the user company and the external partner in a provider company. Furthermore, we observed several business relationships that were intertwined with personal relationships:

> *"Our IT guy is from our region. It's quite convenient, his wife is our general manager. We are all former schoolmates." – UF12, Managing director*

Additionally, trust plays an important role in the information search process as decision-makers often draw on the expertise of a trustee in their personal network rather than solely on provider recommendations or third-party information. Trust with providers can most often only be established through increased personal contact and lengthy or even historical partnerships.

> *"I need to be informed from someone I trust. When I talk to a colleague [CIO in a different company] and I hear 'I've used this and it didn't help at all', it helps me assessing the investment better than if a provider tells me that." – UF-11, CIO*

On the other hand, many providers also attributed the lack of IT security investments to the traditional mindset and overemphasis on the status quo in SME. According to one interviewee, critical assessments of the IT security status quo and subsequent recommendations are even seen as an attack on the user company's self-perception:

> *"In most SME, they don't really have anything [IT security measures] and if we make them aware of this, we are actually the bad guys from their point of view. Because they live in an idyllic world and they don't really want to know about it." – PF-02, Managing director*

Geographical Insularity as a constraint was mentioned in two regards of sourcing: namely sourcing of personnel and service providers. Especially, SME with a more rural location experienced difficulties to attract IT personnel. Furthermore, physical remoteness and thus isolation from providers was seen negatively as it limits sourcing and vendor options. The few experts in rural areas are often fully booked and cannot assist SME regarding IT security decisions, especially if new regulations like the GDPR require many firms to act and invest in external IT security specialists as evidenced by the following statement:

> *"Well, I just talked to the guy who helped set up our computers and works in an IT company. He said 'Pff, you should try to make an appointment with me now because I'll be completely booked out until then' […] and additionally I don't really know whether there are enough IT people who can actually sell and install things. At least not here in our region." – UF-02, Managing director*

Leadership Characteristics

The substantial and highly influential role of top management or leadership in SME has been widely discussed and highlighted in general SME research and was validated during the interviews. Most interviewees agree that the management style or the personality of the managing director or owner have a profound effect on IT security decisions.

Managerial Skills are a prerequisite in most organizational decision-making processes and were thus often mentioned on a more abstract, implicit level. One interviewee, for example, focused on the growing technological complexity which might "overwhelm" especially elder owner-managers – especially compared to their younger entrepreneurial counterparts:

> *"I'd say this is a question of age. I mean, if I have a young entrepreneur in his/her early twenties, s/he approaches the topic differently than someone who is 62. Some people are capable, but others are certainly not." – UF05, Managing director*

Other managers also readily admit that the assessment and evaluation of IT security investments are radically different to those they are used to and thus very burdensome:

"So, I think there is a difference regarding the assessment of whether it is necessary now or not. This is not as easy as with a production machine. There, I know exactly at which hourly rate I can sell the output, so I can calculate an ROI. […] Let's say I buy a firewall and there's an extra feature he [referring to the IT executive] told me about that could provide further security from his point of view. But how do I evaluate that? So, if we can afford it, we'll get it and I feel a bit better. But did we really need it? That is the difficulty with such measures." – UF04, Managing director

Investment decisions are generally directly linked to managerial skills, but some interviewees also mentioned that an inclination towards affinity plays a decisive role regarding IT (security) investments. ***IS/IT Knowledge*** or an owner-manager's disposition towards IT improves leadership inclination to deal with the topic and to provide adequate means for investment:

"Well yes, the main barrier is simply a lack of knowledge!" – UF 06, Managing director

Often paired with the general disposition towards IS/IT is the notion of IT security awareness – both among owner-managers and staff.

"On a scale from 1 to 7 […] I'd position myself on the lower half, because I can do some things myself and regarding other topics, there's an awareness. I just check if and with whom we have to deal with those matters." – UF-12, Managing director

Evidently, managing directors themselves attribute a lot of underinvestment in IT security to the prevalent lack of awareness regarding IT security in general. IT directors and providers regard awareness among top executives as an important prerequisite for the overall awareness in a company.

"This topic of 'raising awareness' is located right at the heart of leadership. Only if they nod, it transcends top-down within the company and you can actually implement it [IT security measures] in the whole company." – PF02, Managing director

Awareness is closely linked to the general ***Attitude and Values*** of the SME leadership. Especially, owner-managers displayed a rather negative, cost-fixated view on IT security investment and dedicated staff as displayed by the following statement:

"[…] in our company it [IT security] is not a job that generates more turnover, i.e., achieves more margin, but simply an in-house administration job that costs me a lot. Of

course, it is clear that you have a few advantages because some things may work better. However, first and foremost, it simply costs money." – UPF01 – Managing director

The direct effect of this unclear "value proposition" of IT in general and IT security in specific, can be evidenced from an IT executive's point of view as follows:

"[…] so we discussed this aspect earlier when we talked about the budget and how difficult it is to get a budget for it [IT security measures] – because at the end of the day, I have a cash outflow with extra resources. So, expenses that are not really visible regarding productivity or revenue. See, when I hire a sales representative or a machine operator who can operate three new machines eight hours a day and deliver more output, it's better to put that into [a productivity] perspective, to argue for it, better than for an IT that just has to run. – UF01, IT director

However, awareness or attitude alone or lack thereof is not the only frequently mentioned leadership constraint. Especially providers explained underinvestment with the temporal focus of leadership on short-term daily business, i.e., the lack of ***Strategic Outlook***. They state that decision-makers in SME rather focus on short-term success and neglect long-term risks for their organizational IT security due to a lack or the neglect of strategic planning:

"Strictly speaking, it's a matter of priorities. I think the priority in SME as of now is on day-to-day operations, on satisfying the demand. Put simply, to keep the daily business running."– PF-04, Business Development

Admittedly, short-term focus plays a significant role in postponing decisions regarding IT security investments. Nevertheless, both interviewees in user and provider companies acknowledge that the highly complex nature of IT security needs to be accounted for. In this line, several managing directors and some CIOs mentioned that they rely heavily on their "gut feeling" due to the lack of information, knowhow, and time for decisions. This demonstrates that decision-makers draw on affective and experiential factors in IT security investment decisions in addition to or rather than on economic modelling or formalized decision support systems.

"You obviously try to calculate the RoI [Return on Investment] but you can easily come up with nice target figures, so I consider it rather 'relative'. This is certainly very important in big enterprises […] It is admittedly not easy to calculate such numbers in the area of security. We do have a decision matrix that we use as an orientation. So, it is not a pure gut decision, but I have to say that gut feeling does play a certain role. We have

hands-on experience with several providers and both play an important role. But we don't have a further formalized decision system." – UPF-02, CIO

All previously identified leadership characteristics were thus found to influence decisions regarding organizational IT security in SME strongly. In the following section, we will discuss our results and their implications for both research and practice.

8.5 Discussion and Implications

The present article identified and described relevant SME constraints in an organizational IT security context and examined how these constraints influence decisions regarding IT security investments in SME. Our findings provide several theoretical contributions and practical implications. From a theoretical perspective, our study validates and contextualizes general SME constraints in organizational IT security and adds to the still prevalent scarcity of qualitative data sources in IS security research. The findings derived from this approach question a variety of assumptions commonly made by studies that implicitly deal with SME as "little big firms". The identified and described constraints help define necessary boundary conditions for future research by challenging and modifying prevalent scholarly explanations (Alvesson & Sandberg, 2011; Rivard, 2014). For instance, common assumptions made in IT security research, like the existence of dedicated personnel and formalized processes, can be denied for a large share of organizations. Overall, the most overlooked or underrepresented assumptions in extant IT security research concern SME constraints of low formalization, insularity, and the strong influence of individual leadership characteristics.

Our findings thus serve as a magnifying glass that exposes non-generalizable assumptions in extant IT security literature and additionally provide guidelines for future research through the analysis of the inferred propositions. These propositions and associated arguments can be seen as a Type II Theory of Explanation (Gregor, 2006) explicating how and why certain constraints influence IT security decisions in SME. Whereas a dominant stream in IT security literature draws on normative decision theories and models like the Return on (Security) Investment or decision theory (Cavusoglu et al., 2008) a descriptive approach that takes into account the manifold influencing factors, e.g., available time, geographical insularity, or individual characteristics, is likely a better lens for organizational IT security investment decisions in SME. In this regard, we contribute to the rather scarce literature on executive and managerial decision-making and investments in an IT security context by pointing out the influence of various characteristics which are possibly highly influential in SME. In addition to the often analyzed lack of

awareness (Hu et al., 2007; Straub & Welke, 1998), the degree of influence and prominence of temporal, experiential, and affective factors in IT security investment decision-making should be included in order to advance our understanding of (under-)investment in SME and the apparent security divide further. Furthermore, other propositions concerning insularity or the small asset base could contribute to exposing neglected or inflated effects in IT security investment decisions and thus contribute to both theory and practice.

Through the juxtaposition of decision-makers – often owner-managers – and employees responsible for IT in user companies and IT security providers, our approach also yielded in several practical implications. By contrasting statements, executives should question themselves whether they overemphasize resource constraints such as limited budget as an "excuse" to delay IT security measures. Even though internal IT staff and providers often acknowledge the existence of resource constraints, they rather contribute a lot of underinvestment to low formalization levels and non-existent budget planning which is an indirect result of prioritizing daily business and the short-term temporal focus of managing directors. Executives in SME can thus learn from our findings that documentation and formalization of processes is a first step that might be time-consuming at first. However, these actions ease the processes of decision-making and leads to fruitful and business-sustaining investments in the long run. Our results also offer several takeaways for providers, such as the importance of lengthy discussions to establish trust-based relationships and the influential role of affective and experiential factors in decision-making processes of their potential customers. Further, large enterprises should consider the role of SME in their value chains more closely. Prominent examples like the Target breach via a third party contractor show that SME can be the gateway to large enterprises for cybercriminals (ZDNet, 2015) or could disrupt certain supply chains in the event of system downtime caused by a severe breach (Cisco, 2018). Dubbed as "the weakest link" in the value chain, large enterprises pressure their SME partner often with additional auditing and quality management tasks rather than pro-actively contributing to an overall secure value chain by supporting their partners. In this regard, expertise provided through partner networks could be highly beneficial since external expertise has been shown to improve SME processes where no knowledge or understanding is readily available (Bradshaw et al., 2013; Cragg et al., 2013). The wish for governmental institutions to provide dedicated and easy to understand support and information was an additional finding during the interview study. Existing support was either not well known or not well-received by many interviewees since the effort to partake in subsidiary schemes or to follow and understand governmental checklists along with other information

sources were deemed excessive for SME. Governments could thus also benefit from our findings and adjust their offers in order to better consider the observed organizational and leadership characteristics.

8.6 Conclusion, Limitations, and Future Research

This study is not without limitations. First, although we employed measures such as data, subject, and researcher triangulation, qualitative research can still be affected by the ambiguity of language or the existence of an elite bias (Fontana & Frey, 2000). Similarly, self-selection bias of the interview partners could be an issue. However, the majority of participants in our sample readily admitted that they had fallen victim to an IT security incident in the past and should thus be representative for the overall SME population (Cisco, 2018). Second, SME should not be considered a homogenous group, especially differences between enterprises in the sector of manufacturing or services have already been noted and discussed. Similarly, very small, small, and medium-sized enterprises are possibly affected by the identified constraints to a varying degree – similarly, startups or SME that employ lean practices and flat hierarchies are likely less prone to suffer from the same disadvantages of a low formalization level or lacking IT/IS skills and knowledge of the owner-manager. Overall, the proposed constraints and their influence in IT security investment should rather be seen on a continuum influencing SME depending on organizational size, IT staff, or industry. Furthermore, our results might be affected by our sample choice as our interviewees are all based in one West European country. However, previous organizational SME research has shown comparable patterns of SME characteristics and constraints across national borders and cultures (Chen et al., 2007; Dutta & Evrard, 1999; Thong, 2001).

Nevertheless, future research could build on our findings with an international comparison utilizing quantitative measures to determine the effect size of SME constraints on IT security decisions. Additionally, prospective studies should analyze industries other than healthcare and financial institutions as many of the extant results are hardly generalizable and test the postulated propositions in both an SME and a large enterprise context for more nuanced findings and recommendations (Kam et al., 2019). Another avenue for future studies, could be a further partition of the SME context into very small, small, and medium-sized enterprises and to measure and compare the degree of prominence of identified constraints empirically.

8.7 Acknowledgments

An earlier version of this article was presented at the International Conference of Information Systems (ICIS) 2018 and appeared in the subsequent proceedings of ICIS 2018 under the title “The Influence of SME Constraints on Organizational IT Security”.

9 Thesis Contributions and Conclusion

The goal of this dissertation was to improve the understanding of decision-making processes in organizations regarding cloud computing adoption, data protection behavior, and IT security measures—decisions that most organizations are faced with when undergoing digital transformation development. Particular emphasis was placed on factors influencing the decision-making of managers and other important organizational decision-makers. Additionally, one study investigated how feelings of psychological ownership might influence behavioral intention and decisions, depending on whether the study subject intended to protect data in a personal or in a professional context. Drawing on findings of behavioral economists, the findings also suggest that decisions in an organizational context do not adhere (fully) to the tenets postulated by rational choice theory. Decision-makers are influenced, rather, by a plethora of economic, environmental, behavioral, and organizational factors as explicated in further detail in the following sections.

Additionally, this dissertation sheds light on under-researched areas in information systems, such as the adoption of and investment in IT security measures in SMEs. Whereas previous technology adoption research—for example, regarding e-commerce or e-business (Stockdale & Standing, 2006; Worrall et al., 2005)—has already provided evidence of potential inhibitors and enablers in SMEs, only one dedicated study exists in an IT security context (Lee & Larsen, 2009). In this regard, especially the latter two studies described in Papers D and E provide several key insights and avenues for future research that account for the structural differences of SMEs and the specific characteristics of decision-makers in SMEs that influence IT security investment decisions.

Based on the five featured studies, this dissertation significantly contributes to the understanding of influencing factors in decision-making processes in general and highlights constraints and characteristics specific to small and medium-sized enterprises.

In the remainder of this section, theoretical contributions and practical implications are described in more detail. Subsequently, a conclusion provides propositions for future research and completes the dissertation.

9.1 Theoretical Contributions

The first two studies of this dissertation (i.e., Papers A and B) followed a deductive approach, studying two specific phenomena influencing decision-making processes regarding cloud computing adoption and data protection behavior.

Paper A validates that status quo thinking can impede the adoption of new technological systems, such as SaaS. Especially, decision-makers who cannot draw on prior experience with SaaS are overestimating risks associated with its adoption, thereby exemplifying the impact of status quo thinking and leading to retention of the incumbent system. Therefore, the paper illustrates the significant influence of reference-dependence in line with prospect theory rather than rational choice theory (Kahneman & Tversky, 1979; Levy, 1992, 1997). Additionally, this study was the first at the time of publishing to draw on prospect theory when analyzing managers' appraisal of SaaS in an organizational context based on their evaluation of the respective incumbent technology. As such, this study also provides the first evidence that the effect of status quo thinking is more pronounced for decision-makers with lower experience levels by measuring the bias indirectly at the group level rather than through an explicit indicator based on self-assessment on an individual level (e.g., perceived sunk costs as in Polites and Karahanna 2012). These findings are especially valuable, since a large part of technology adoption decisions that decision-makers are faced with during digital transformation processes are, in fact, replacement decisions. Therefore, future research should account for the effect of incumbent technology systems when studying attitudinal beliefs and adoption decisions regarding technologies potentially succeeding them.

Paper B also contributes to the understanding of how non-rational factors such as feelings can affect decision-making in various contexts. By drawing on the concept of psychological ownership—a concept only scarcely investigated in IS or in the specific data protection scenario of this study—the findings suggest that psychological ownership does significantly influence several protection motivation antecedents only in the private context. The longitudinal repeated measures approach reveals that psychological ownership comes only marginally into effect in the professional context. By employing such a research design, this study was the first at the time of publishing that employed such a comparison of the same data protection behavior in two different contexts. Additionally, the study implies that findings of other studies performed solely in one of these contexts are not necessarily applicable in the other context or are generalizable. Regarding the underlying theoretical framework of the protection motivation theory, findings also indicate that risk perception in isolation does not promote data protection

measures in any context. The findings do suggest, however, that controllability has a significant effect and could contribute to a more thorough understanding of the intention of employees to use strong passwords as a measure to protect data.

The second part of this thesis (i.e., Papers C, D, and E) critically investigates how information systems research regarding IT security approaches the decision-making process while placing particular emphasis on decision-makers in small and medium-sized enterprises.

Paper C confirms that decision-making processes regarding IT security measures are affected by various contextual aspects instead of purely rational decision-making. As already demonstrated in Paper A, decision-makers are faced with a highly complex decision as IT security investments draw on a variety of heuristics and biases and take a multitude of external factors into account. Extant research, however, largely disregards these influencing factors and still heavily relies on normative approaches like rational choice theory, as demonstrated by the analysis of prior IT security research. The findings of a qualitative study, triaged with the results of the literature review, also uncover several areas that remain largely overlooked. Furthermore, the study implies that the IT security decision process should be regarded in a more nuanced manner, in other words, whether the decision-maker should decide the level of investment, its source or area, or whether the IT security investment should be considered at all. The latter nuance is particularly important in an SME context, as demonstrated in *Paper C* and the following two papers.

In this regard, *Paper D* offers a conceptual framework of SME constraints that displays how characteristics of the focal SME, their micro- and macro-environment, are based on a literature analysis of existing SME research. These constraints are contextualized regarding IT security investment in SMEs. The study finds that limited resources, a small asset base, low formalization levels, insularity, and leadership styles are all manifested and exert an effect on organizational IT security. The perceived amplitude of the effects, however, varies according to the roles of the interviewed decision-makers and whether they are representing a user or a provider firm. This juxtaposition of decision-makers demonstrates that managing directors emphasize the constraining effect of limited resources and admit that the short-term temporal focus—as well as affective or experiential factors, such as the previously mentioned “gut feeling”—play an important role in decision-making processes. Decision-makers stemming from IT departments or providers, however, consider other constraints to be highly relevant, including the low formalization level of processes or budget planning as well as a lack of awareness. Since the majority of prior IT security studies largely neglected the “SME reality” and did not account for these

constraints acting as potential boundary conditions, extant findings should thus be challenged or should be modified accordingly. Additionally, the study provides guidelines for future research through the analysis of 14 derived propositions and by exposing non-generalizable assumptions in extant IT security literature. Categorized as a type II theory of explanation (Gregor, 2006), describing how and why certain constraints influence IT security decisions in SMEs, the study also implies the importance of a descriptive approach—in contrast to the dominant stream in IT security research drawing on normative decision theories.

Paper E further expands the findings of Paper D and offers a more detailed literature analysis and conceptual framework explicating the reason behind the security divide between SMEs and large enterprises. This conceptual framework displaying SME characteristics and constraints helps define necessary boundary conditions for future research (Alvesson & Sandberg, 2011; Rivard, 2014). The study finds that the most underrepresented boundary conditions affecting SMEs in extant IT security research are the low levels of formalization and procedural sophistication, insularity, and the strong influence of individual characteristics of SME executives. Moreover, Paper E—like Paper D—adds to the still-prevalent scarcity of qualitative studies in IS security in general and represents one of the few SME-focused data sources in this research field. Future studies can, therefore, build on the study and challenge or even modify prevalent scholarly explanations for the security divide. Besides the quite extensively researched lack of security awareness of employees and management, Paper E highlights the importance and impact of further temporal, experiential, and affective factors in IT security investment decision-making.

9.2 Practical Implications

In addition to the above-discussed theoretical contributions, the studies and this dissertation also offer several practical implications that are examined subsequently.

Paper A offers implications for both SaaS providers and potential new adopters. The findings imply that decision-makers should be aware of decision biases such as status quo thinking and reference-dependence affecting their decision-making. The new SaaS technology should not only be compared to the incumbent system but also evaluated as a standalone solution. When faced with such a replacement choice, decision-makers should actively seek out more experience through workshops, trials, or lighthouse projects.

These recommendations are also of interest for providers: Non-adopters, especially, will likely require more facts and hands-on experience with the new product, and sales or marketing communication should be altered accordingly. Another interesting takeaway for providers is that their existing client base will likely require less persuasion, which allows for further capitalization via horizontal or vertical system integrations. Furthermore, these first adopters could be beneficial in convincing inexperienced prospects. Organizing roundtable discussions with existing customers or displaying customer success stories can exert social influence on the risk assessment of inexperienced decision-makers and, ultimately, decrease their level of uncertainty as well as highlight financial or strategic advantages.

Paper B is of practical importance, since it reveals that psychological ownership does, indeed, influence an individual's intention to protect data, however, only in a private context. Nevertheless, these findings suggest that practitioners could instill feelings of psychological ownership in employees who should use strong passwords as a safeguarding mechanism to protect data in a professional context. By stimulating the antecedents of psychological ownership, such as a deep understanding of the sensitivity of the data in a professional context, employees feel higher degrees of association with the data, which in turn motivates safeguarding behavior. Similarly, investing resources (such as time or effort) into the creation of data also facilitates feelings of ownership. Organizational stakeholders in IT security could, therefore, ensure that employees who deal with the data better understand the content, so that they see data in a professional context as a reflection of their own data. Enabling employees to choose and employ safeguarding measures—for example, offering a choice of password managers and fully explaining the use of such—could increase their feelings of freedom of choice, accountability, and controllability, which was demonstrated to influence protection motivation.

The remaining studies focus on IT security investment decisions and the possible factors influencing these decisions.

Paper C offers insight in the nuances of the decision. IT security investment decisions are often either directed at the level, source, or area of the investment, or decision-makers evaluate whether to invest at all. Consequently, providers of IT security measures should account for these nuances and adapt the value proposition of their product or service accordingly. Additionally, decision-makers in SMEs do not necessarily employ economic tools and methods like ROSI estimations due to resource constraints, but rather rely on their intuition and analyze only costs rather than benefits of a possible IT security investment. Furthermore, environmental aspects—for example, being forced to adhere to IT security standards due to auditing pressure as

a supplier of large enterprises—strongly influence the decision to invest in IT security. Decision-makers are more likely to invest in IT security measures when their business relationships are at risk. Compliance with such externally established IT security pressures—or state interventions such as the GDPR and the possibility of sanctions—is a strong motivator for SME decision-makers. This offers interesting insights to IT security providers, state regulators, and supply chain partners. However, state regulators should not rely solely on sanctions but rather should encourage SME decision-makers to view IT security measures as a potential economic opportunity to increase customer acquisition, loyalty, and satisfaction.

Paper D and *Paper E* highlight the specific situation of small and medium-sized enterprises when faced with IT security investment decisions. The analysis and juxtaposition of SME decision-makers, who are often owner-managers, and employees responsible for IT and IT security offered several practical implications and insights into perceptual differences. Whereas owner-managers or SME executives often point to budgetary and time constraints, IT staff and providers regard resource constraints as an easily stated excuse and attribute low IT security investment levels to a lack of procedural sophistication or even the absence of any budget planning. The findings in these studies suggest that formalizing and documenting existing business and IT processes can be a fruitful, albeit time-consuming, first approach to decreasing the security divide. Improving formalization levels can also contribute to easing decision-making. Managing directors, SME executives, or owner-managers should be aware of their prioritization of daily business and their short-term temporal focus and how this focus might obstruct business-sustaining investment. Paper D and Paper E also offer interesting insights for providers of IT security products and services: Lengthy discussions might be necessary to establish relationships based on trust, due to the pronounced influence of affective and experiential factors in decision-making within SMEs. Since trust is often based on experience, SMEs and the value chains of which they are a part can also benefit from partner networks or roundtable sessions established or joined by large enterprises. Because security levels at SMEs are important for large enterprises that often audit SMEs as their suppliers, providing access to their IT security knowledge, expertise, and in-house experience can benefit all stakeholders. The studies also find that regulatory actions are often regarded as negative or detrimental—especially consequences and sanctions connected to the GDPR—whereas governmental support was largely seen as cumbersome or was relatively unknown. Providing easy-to-understand and quick-to-apply-for governmental support was mentioned frequently. Therefore, governments should reconsider the way IT security grants and subsidies are advertised and can be claimed. Leveraging local institutions like chambers of commerce and offering subsidiary schemes along

with checklists that are easy to follow and understand could benefit overstrained SME executives and increase the general level of IT security. All of these measures, therefore, could reduce the security divide between SMEs and large enterprises.

Since their publication, several of the above-mentioned theoretical and practical findings have informed and influenced subsequent IS and organizational psychology research (Dwivedi et al., 2020; Hintsch & Turowski, 2019; Iannacci et al., 2020; Olt et al., 2019).

9.3 Conclusion and Future Research

Digital transformation is omnipresent—the term itself is even increasingly regarded as a buzzword—but the ramifications of digital transformation on individuals and society as a whole, as well as on the economy and regulatory bodies, merit the increased research intensity this topic has received. Interestingly, the introductorily cited Warren McFarlan—who is widely credited as the first graduate in information systems and who co-wrote the first book on the management of IS in 1966—argues exactly 50 years later that, despite the increasing complexity of managing technology, managers continue to face and endure the same issues year after year. Five decades of case-study research and serving as the third editor-in-chief of the MISQ journal have corroborated that there is, in fact, "always a new technology […] but underlying it, there are some basic management principles" (McFarlan, 2016).

As outlined in the introduction of this dissertation and throughout the constituent research studies, decision-making processes lie at the heart of digital transformation: All changes regarding the famous transformation triad of "people, process, technology" require a decision made, either by an individual within an organization or a group of stakeholders. Therefore, when analyzing management principles, we must focus on underlying decision-making processes.

Following findings from behavioral science, individuals or groups who are tasked with managing—in other words, with making decisions—are highly affected by an array of influencing factors during their decision-making or problem-solving process, and they do not behave as fully rational human actors. The studies featured in this dissertation encompassed various IT artifacts and focused on various stakeholders within organizations to answer the five research questions introduced in Chapter 1.2. The findings of these studies suggest that heuristics, biases, and emotions play decisive roles in data protection behavior and the adoption of new IT systems based on cloud computing. Based on the analysis of managers and IT executives, the first study finds that status quo thinking, indeed, influences managers' decisions in adopting new SaaS IT

systems. Managers “circumvent” their lack of information or experience with a new SaaS solution by drawing on a reference point constituted by their existing, incumbent IT systems. The less experienced they are regarding cloud-based solutions, the stronger their dependence on their experience with familiar technologies. The evaluation of the new technology relies heavily on their assessment of the existing one.

Focusing on a different IT artifact, password protection behavior to secure private or organizational data, the second study of this dissertation focused on how psychological ownership affects the decision to protect data. Compared to the first and the following studies, this study does not focus solely on the top echelon’s assessment but also contrasts decision-making behavior in two different situational contexts. Since the feeling of psychological ownership positively and significantly influences the attitude toward data protection in a private context, fostering this feeling in a professional context might result in an uptake of data protection measures. Future research could analyze the antecedents of psychological ownership in a professional context and test its effect through experiments and action research.

Whereas the first studies predominantly focused on behavioral and cognitive aspects, the remaining studies aimed at a more holistic approach to identify influencing factors in IT security decisions. The results of the third study included in this dissertation suggest that decision-makers in small and medium-sized enterprises are influenced by a wide array of aspects during decision-making processes regarding organizational IT security. The extensive literature review demonstrated, however, that several aspects are strongly disregarded in existing IS research. Therefore, future research could fill the identified research gaps, for example, regarding sourcing decisions or initial adoption decisions. One major finding of this study and a highlighted avenue for future studies was the scarcity of SME-focused research in organizational IT security decisions. The fourth and fifth studies concluding this dissertation tap into this research gap and focus on how SME characteristics or constraints influence IT security investment decisions in small and medium-sized enterprises. Based on in-depth interviews with decision-makers, these studies find that decisions regarding organizational IT security in SMEs are strongly affected by SME-specific characteristics. These include the low formalization levels of processes or the multitude of roles exemplified by owner-managers who are in charge of both strategic decisions affecting business continuance and operational tasks as well as deeply involved with the day-to-day business. Comparing the degree of prominence of these and further identified constraints and their roles in decision-making could be an interesting next step for researchers

interested in SMEs and their adoption of security measures or digital applications and processes.

Apart from the already-stated ideas for future research, it is hoped that the derived results of this dissertation will inspire further research and provide insights and practical suggestions for individual and organizational decision-makers, regulatory bodies, and providers of cloud computing software and data protection or IT security measures. Especially valued would be longitudinal studies that do not simply capture a "snapshot in time" but re-evaluate decision-making behavior over time and could provide further insights into decision-making in times of digital transformation. Additionally, findings in this dissertation are based on European samples and should thus be verified or replicated in different cultural and legal settings. Due to the strong focus on SME decision-makers, the featured studies and their results were derived from individual decision-making processes. Analysis of group decision-making and how cognitive biases, contextual aspects, or constraints affect groups in contrast to individuals also merits research attention.

Nevertheless, these findings highlight the fact that decision-making processes in times of constant change, where previous experience or resources are scarce, do not adhere to the tenets postulated by rational choice theory. Decision-makers in SMEs especially rely on other factors and are bounded by constraints such as firm characteristics and external pressures and barriers. Since IS research covers decision-making processes regarding ubiquitous computing, virtual environments, and digital transformation—as well as the resulting consequences on individuals, business, and society—the application of methods and findings of behavioral scientists can inform IS research and advance related disciplines (Crossler et al., 2013; Goes, 2013). In this regard, IS can be repositioned as a reference discipline in its own right, which informs and is in a discourse with other disciplines (Baskerville & Myers, 2002).

References

Adomavicius, G., Bockstedt, J. C., Gupta, A., & Kauffman, R. J. (2008). Making Sense of Technology Trends in the Information Technology Landscape. *MIS Quarterly*, *32*(4), 779–809.

Agell, J. (2004). Why are Small Firms Different? Managers' Views. *Scandinavian Journal of Economics*, *106*(3), 437–453.

AIS. (2018). *Senior Scholars' Basket of Journals*. https://aisnet.org/page/SeniorScholarBasket Accessed 26 January 2018.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Ajzen, I. (2002). Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior. *Journal of Applied Social Psychology*, *32*(4), 665–683.

Ajzen, Icek. (1985). *From Intentions to Actions: A Theory of Planned Behavior*. Springer Berlin Heidelberg.

Ajzen, Icek, & Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behaviours*. Prentice Hall.

Albrechtsen, E. (2007). A Qualitative Study of Users' View on Information Security. *Computers & Security*, *26*(4), 276–289.

Altinkemer, K., & Wang, T. (2011). Cost and Benefit Analysis of Authentication Systems. *Decision Support Systems*, *51*(3), 394–404.

Alvesson, M., & Sandberg, J. (2011). Generating Research Questions through Problematization. *Academy of Management Review*, *36*(2), 247–271.

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613–643.

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. *MIS Quarterly*, *41*(3), 893–916.

Aral, S., & Walker, D. (2011). Creating Social Contagion through Viral Product Design: A Randomized Trial of Peer Influence in Networks. *Management Science, 57*(9), 1623–1639.

Arendt, L. (2008). Barriers to ICT Adoption in SMEs: How to Bridge the Digital Divide? *Journal of Systems and Information Technology*, *10*(2), 93–108.

Armstrong, J. S., & Overton, T. S. (1977). Estimating Nonresponse Bias in Mail Surveys. *Journal of Marketing Research*, *14*(3), 396–402.

Auerbach, C., & Silverstein, L. B. (2003). *Qualitative Data: An Introduction to Coding and Analysis*. New York University Press.

Avey, J. B., Avolio, B. J., Crossley, C. D., & Luthans, F. (2009). Psychological Ownership: Theoretical Extensions, Measurement and Relation to Work Outcomes. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior*, *30*(2), 173–191.

Bagozzi, R. P., & Yi, Y. (1989). On the Use of Structural Equation Models in Experimental Designs. *Journal of Marketing Research*, *26*(3), 271–284.

Bagozzi, R. P., & Yi, Y. (2012). Specification, Evaluation, and Interpretation of Structural Equation Models. *Journal of the Academy of Marketing Science*, *40*(1), 8–34.

Bagozzi, Richard P., & Yi, Y. (1988). On the Evaluation of Structural Equation Models. *Journal of the Academy of Marketing Science*, *16*(1), 74–94.

Baker, W. H., Rees, L. P., & Tippett, P. S. (2007). Necessary Measures—Metric-driven Information Security Risk Assessment and Decision-Making. *Communications of the ACM*, *50*(10), 101–106.

Bakos, J. Y., & Kemerer, C. F. (1992). Recent Applications of Economic Theory in Information Technology Research. *Decision Support Systems*, *8*(5), 365–386.

Ballantine, J., Levy, M., & Powell, P. (1998). Evaluating Information Systems in Small and Medium-sized Enterprises: Issues and Evidence. *European Journal of Information Systems*, *7*, 241–251.

Bamberger, P., & Fiegenbaum, A. (1996). The Role of Strategic Reference Points in Explaining the Nature and Consequences of Human Resource Strategy. *Academy of Management Review*, *21*(4), 926–958.

Bandara, W., Miskon, S., & Fielt, E. (2011). *A Systematic, Tool-supported Method for Conducting Literature Reviews in Information Systems*. Proceedings of the19th European Conference on Information Systems (ECIS), Helsinki, Finland.

Bandura, A. (1997). Self-Efficacy: Toward a Unifying Theory of Behavioral Change. *Psychological Review*, *84*, 191–215.

Barnard, L., & Solms, R. von. (2000). A Formalized Approach to the Effective Selection and Evaluation of Information Security Controls. *Computers & Security*, *19*(2), 185–194.

Barrett, B. (2019). *Hack Brief: An Astonishing 773 Million Records Exposed in Monster Breach*. https://www.wired.com/story/collection-one-breach-email-accounts-passwords/ Accessed 20 January 2019.

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information System Security Commitment: A Study of External Influences on Senior Management. *Computers & Security*, *59*, 9–25.

Baskerville, R. (1989). Logical Controls Specification: An Approach to Information Systems Security. In H. K. Klein & K. Kumar (Eds.), *Systems Development for Human Progress* (pp. 241–255). Elsevier Science Publishers.

Baskerville, R. (1991). Risk Analysis: An Interpretative Feasibility Tool in Justifying Information Systems Security. *European Journal of Information Systems*, *1*(2), 121–130.

Baskerville, R., & Myers, M. D. (2002). Information Systems as a Reference Discipline. *Management Information Systems Quarterly*, *26*(1), 1–14.

Baskerville, Richard. (1991). Risk Analysis as a Source of Professional Knowledge. *Computers & Security*, *10*(8), 749–764.

Baskerville, Richard. (1993). Information Systems Security Design Methods: Implications for Information Systems Development. *ACM Computing Surveys (CSUR)*, *25*(4), 375–414.

Bassellier, G., Reich, B. H., & Benbasat, I. (2001). Information Technology Competence of Business Managers: A Definition and Research Model. *Journal of Management Information Systems*, *17*(4), 159–182.

Bazeley, P. (2003). Computerized Data Analysis for Mixed Methods Research. In A. Tashakkori & C. Teddlie (Eds.), *Handbook of Mixed Methods in Social & Behavioral Research* (pp. 385–422). SAGE.

Bazerman, M. H. M. (2008). *Judgement in Managerial Decision Making* (Vol. 7). Wiley.

Beck, T., & Demirguc-Kunt, A. (2006). Small and Medium-size Enterprises: Access to Finance as a Growth Constraint. *Journal of Banking & Finance*, *30*(11), 2931–2943.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, *11*(3), 369–386.

Benbasat, I., & Zmud, R. W. (1999). Empirical Research in Information Systems: The Practice of Relevance. *MIS Quarterly*, *23*(1), 3–16.

Benlian, A. (2009). *A Transaction Cost Theoretical Analysis of Software-as-a-Service (SAAS)-based Sourcing in SMBs and Enterprises*. Proceedings of the 17th European Conference in Information Systems (ECIS), Verona, Italy.

Benlian, A., & Hess, T. (2010). *The Risks of Sourcing Software as a Service-An Empirical Analysis of Adopters and Non-Adopters*. Proceedings of the 18th European Conference on Information Systems (ECIS), Pretoria, South Africa.

Benlian, A., & Hess, T. (2011). Opportunities and Risks of Software-as-a-Service: Findings from a Survey of IT Executives. *Decision Support Systems*, *52*(1), 232–246.

Benlian, A., Hess, T., & Buxmann, P. (2009). Drivers of SaaS-Adoption – An Empirical Study of Different Application Types. *Business & Information Systems Engineering*, *1*(5), 357–369.

Bennett, R., & Robson, P. J. A. (2004). The Role of Trust and Contract in the Supply of Business Advice. *Cambridge Journal of Economics*, *28*(4), 471–489.

Bharati, P., & Chaudhury, A. (2009). SMEs and Competitiveness: The Role of Information Systems. *Management Science and Information Systems Faculty Publication Series*, *15*, i–ix.

Birley, S. (1982). Corporate Strategy and the Small Firm. *Journal of General Management*, *8*(2), 82–86.

Bodin, L. D., Gordon, L. A., & Loeb, M. P. (2005). Evaluating Information Security Investments Using the Analytic Hierarchy Process. *Communications of the ACM*, *48*(2), 79–83.

Bogdan, R. C., & Biklen, S. K. (2007). *Qualitative Research for Education: An Introduction to Theories and Methods* (Vol. 5). Pearson Education.

Bornstein, R. F. (1989). Exposure and Affect: Overview and Meta-Analysis of Research, 1968-1987. *Psychological Bulletin*, *106*(2), 265–289.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. M., & Polak, P. (2015). What do Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Behaviors in Users. *MIS Quarterly*, *39*(4), 837–864.

Boyes, J., & Irani, Z. (2003). *Barriers and Problems Affecting Web Infrastructure Development: The Experiences of a UK Small Manufacturing Business*. Proceedings of the 9th Americas Conference on Information Systems (AMCIS), Tampa, USA 724–732.

Bradshaw, A., Cragg, P., & Pulakanam, V. (2013). Do IS Consultants Enhance IS Competences in SMEs? *Electronic Journal of Information Systems Evaluation*, *16*(1), 1–23.

Brunel, F. F., Tietje, B. C., & Greenwald, A. G. (2004). Is the Implicit Association Test a Valid and Valuable Measure of Implicit Consumer Social Cognition? *Journal of Consumer Psychology*, *14*(4), 385–404.

BS 7799-1:1995. (1995). *Information Security Management. Code of Practice for Information Security Management Systems*.

Buckley, P. J. (1997). International Technology Transfer by Small and Medium-sized Enterprises. *Small Business Economics*, *9*(1), 67–78.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness. *MIS Quarterly*, *34*(3), 523–548.

Business Week. (1990). *Is Research in the Ivory Tower 'Fuzzy, Irrelevant, Pretentious? October 29*, 62–66.

Busse, J., Humm, B., Lübbert, C., Moelter, F., Reibold, A., Rewald, M., Schlüter, V., Seiler, B., Tegtmeier, E., & Zeh, T. (2014). Was bedeutet eigentlich Ontologie? *Informatik Spektrum*, *37*, 289–297.

Caldeira, M. M., & Ward, J. M. (2003). Using Resource-Based Theory to Interpret the Successful Adoption and Use of Information Systems and Technology in Manufacturing Small and Medium-sized Enterprises. *European Journal of Information Systems*, *12*(2), 127–141.

Camerer, C. F. (2003). Strategizing in the Brain. *Science*, *300*(5626), 1673–1675.

Carbo-Valverde, S., Rodriguez-Fernandez, F., & Udell, G. F. (2007). Bank Market Power and SME Financing Constraints. *Review of Finance*, *13*(2), 309–340.

Casterella, J. R., Francis, J. R., Lewis, B. L., & Walker, P. L. (2004). Auditor Industry Specialization, Client Bargaining Power, and Audit Pricing. *Auditing: A Journal of Practice & Theory*, *23*(1), 123–140.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A Model for Evaluating IT Security Investments. *Communications of the ACM*, *47*(7), 87–92.

Cavusoglu, H., Raghunathan, S., & Cavusoglu, H. (2009). Configuration of and Interaction Between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems. *Information Systems Research*, *20*(2), 198–217.

Cavusoglu, Huseyin, Cavusoglu, H., Son, J.-Y., & Benbasat, I. (2015). Institutional Pressures in Security Management: Direct and Indirect Influences on Organizational Investment

in Information Security Control Resources. *Information & Management, 52*(4), 385–400.

Cavusoglu, Huseyin, Raghunathan, S., & Yue, W. T. (2008). Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems, 25*(2), 281–304.

Chang, K. C., & Wang, C. P. (2011). Information Systems Resources and Information Security. *Information Systems Frontiers, 13*(4), 579–593.

Chase, V. M., Hertwig, R., & Gigerenzer, G. (1998). Visions of Rationality. *Trends in Cognitive Sciences, 2*(6), 206–214.

Chau, P. Y. K. (1996). An Empirical Assessment of a Modified Technology Acceptance Model. *Journal of Management Information Systems, 13*(2), 185–204.

Chell, E., Haworth, J. M., & Brearley, S. A. (1991). *The Entrepreneurial Personality. Concepts, Cases, and Categories* (Vol. 1). Routledge.

Chen, H., Lee, M., & Wilson, N. (2007). *Resource Constraints Related to Emerging Integration Technologies Adoption: The Case of Small and Medium-Sized Enterprises*. Proceedings of the 13th Americas Conference on Information Systems (AMCIS), Keystone, USA.

Chen, P., Kataria, G., & Krishnan, R. (2011). Correlated Failures, Diversification, and Information Security Risk Management. *Management Information Systems Quarterly, 35*(2), 387–422.

Cichy, P., Salge, T. O., & Kohli, R. (2014). *Extending the Privacy Calculus: The Role of Psychological Ownership*. Proceedings of the 35th International Conference on Information Systems (ICIS), Auckland, New Zealand.

Cisco. (2016). *Cisco Global Cloud Index: Forecast and Methodology, 2015–2020.* https://www.cisco.com/c/dam/m/en_us/service-provider/ciscoknowledgenetwork/files/622_11_15-16-Cisco_GCI_CKN_2015-2020_AMER_EMEAR_NOV2016.pdf Accessed 11 November 2016.

Cisco. (2018). *Small and Mighty—How Small and Midmarket Businesses Can Fortify Their Defenses Against Today's Threats*. https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf. Accessed 20 February.

Coden, M., Madnick, S., Pentland, A., & Yousuf, S. (2016). *How to Prepare for the Cyberattack that is Coming to your Company*. https://www.cio.com/article/3185725/security/9-biggest-information-security-threats-through-2019.html Accessed 10 February 2019.

Coden, M., Madnick, S., Pentland, A., & Yousuf, S. (2019). *How to Prepare for the Cyberattack that is Coming to your Company*. https://www.weforum.org/agenda/2016/11/how-to-prepare-for-the-cyberattack-that-is-coming-to-your-company/ Accessed February 10 2020.

Cooper, H. M. (1988). Organizing Knowledge Syntheses: A Taxonomy of Literature Reviews. *Knowledge in Society*, *1*(1), 104–126.

Cragg, P., Caldeira, M., & Ward, J. (2011). Organizational Information Systems Competences in Small and Medium-sized Enterprises. *Information & Management*, *48*(8), 353–363.

Cragg, P., Mills, A., & Suraweera, T. (2013). The Influence of IT Management Sophistication and IT Support on IT Success in Small and Medium-sized Enterprises. *Journal of Small Business Management*, *51*(4), 617–636.

Craig-Wood, K. (2010). *Definition of Cloud Computing, Incorporating NIST and G-Cloud Views*. KatesComment. http://www.katescomment.com/definition-of-cloud-computing-nist-g-cloud/ Accessed 15 December 2019

Creswell, J. W. (1998). *Qualitative Inquiry and Research Design: Choosing Among Five Traditions*. Sage.

Crossler, R. E. (2010). *Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data*. Proceedings of the 43rd Annual Hawaii International Conference on System Sciences (HICSS), Kauai, USA.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future Directions for Behavioral Information Security Research. *Computers & Security*, *32*, 90–101.

Dahlberg, T., Kivijärvi, H., & Saarinen, T. (2017). *Longitudinal Study on the Expectations of Cloud Computing Benefits and an Integrative Multilevel Model for Understanding Cloud Computing Performance.* 50th Hawaii International Conference on System Sciences (HICSS), Big Island, USA.

Das, T., & Teng, B. K. (1999). Cognitive Biases and Strategic Decision Processes: An Integrative Perspective. *Journal of Management Studies*, *36*(6), 757–778.

David, P. A. (1985). Clio and the Economics of QWERTY. *The American Economic Review*, *75*(2), 332–337.

Davis, F. D. (1986). *A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results*. Massachusetts Institute of Technology, Sloan School of Management.

Davison, R. M., & Martinsons, M. G. (2016). Context is King! Considering Particularism in Research Design and Reporting. *Journal of Information Technology*, *31*(3), 241–249.

Decker, M., Schiefer, G., & Bulander, R. (2006). *Specific Challenges for Small and Medium-sized Enterprises (SME) in M-Business*. Proceedings of the International Conference on E-Business (ICE-B 2006),Setúbal, Portugal, 169–174.

Dhillon, G. (1997). *Managing Information System Security*. Macmillan.

Dhillon, G., & Backhouse, J. (2001). Current Directions in IS Security Research. Towards Socio-organizational Perspectives. *Information Systems Journal*, *11*(2), 127–153.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused Assessment of Information System Security in Organizations. *Information Systems Journal*, *16*(3), 293–314.

Dholakia, R. R., & Kshetri, N. (2004). Factors Impacting the Adoption of the Internet among SMEs. *Small Business Economics*, *23*(4), 311–322.

Dibbern, J. (2004). *The Sourcing of Application Software Services. Empirical Evidence of Cultural, Industry and Functional Differences*. Physica-Verlag.

Dipboye, R. L. (1977). A Critical Review of Korman's Self-Consistency Theory of Work Motivation and Occupational Choice. *Organizational Behavior and Human Performance*, *18*, 108–126.

Dittmar, H. (1992). *The Social Psychology of Material Possessions: To Have Is to Be*. Hemel Hampstead, Harvester Wheatsheaf and St Martin's Press.

Dojkovski, S., Lichtenstein, S., & Warren, M. J. (2007). *Fostering Information Security Culture in Small and Medium Size Enterprises: An Interpretive Study in Australia*. In: Proceedings of the 15th European Conference on Information Systems (ECIS), St. Gallen, 1560–1571.

Dor, D., & Elovici, Y. (2016). A Model of the Information Security Investment Decision-Making Process. *Computers & Security*, *63*, 1–13.

Drechsler, A., & Weißschädel, S. (2018). An IT Strategy Development Framework for Small and Medium Enterprises. *Information Systems and E-Business Management*, *16*(1), 93–124.

Duncan, N. G. (1981). Home Ownership and Social Theory. In J. S. Duncan (Ed.), *Housing and Identity: Cross-Cultural Perspectives* (pp. 98–134). Croom Helm.

Dutta, A., & Roy, R. (2008). Dynamics of Organizational Information Security. *System Dynamics Review*, *24*(3), 349–375.

Dutta, S., & Evrard, P. (1999). Information Technology and Organisation within European Small Enterprises. *European Management Journal*, *17*(3), 239–251.

Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, M. D. (2017). Re-examining the Unified Theory of Acceptance and Use of Technology (UTAUT): Towards a Revised Theoretical Model. *Information Systems Frontiers*, 1–16.

Dwivedi, Y. K., Rana, N. P., Tamilmani, K., & Raman, R. (2020). A Meta-Analysis based Modified Unified Theory of Acceptance and Use of Technology (Meta-UTAUT): A Review of Emerging Literature. *Current Opinion in Psychology*, *36*, 13–18.

Eduserv. (2015). *Government, Technology and the Language of Business Change*. https://www.eduserv.org.uk/~/media/Insight/Reports/WEB1490%20Government%20technology%20and%20the%20language%20of%20business%20change.pdf Accessed 11 November 2016.

Eikebrokk, T. R., & Olsen, D. H. (2007). An Empirical Investigation of Competency Factors affecting E-Business Success in European SMEs. *Information & Management*, *44*(4), 364–383.

Ekenberg, L., Oberoi, S., & Orci, I. (1995). A Cost Model for Managing Information Security Hazards. *Computers & Security*, *14*(8), 707–717.

El-Gayar, O. F., & Fritz, B. D. (2010). A Web-based Multi-perspective Decision Support System for Information Security Planning. *Decision Support Systems*, *50*(1), 43–54.

European Commission. (2003). *Commission Recommendation of 6 May 2003 Concerning the Definition of Micro, Small and Medium-sized Enterprises (notified under Document Number C(2003) 1422)*. Official Journal of the European Union 46 (L 124).

Eurostat. (2014). *ICT Usage in Enterprises in 2014: Cloud Computing Services Used by One Out of Every Five Enterprises in the EU28*. http://ec.europa.eu/eurostat/documents/2995521/6208098/4-09122014-AP-EN.pdf Accessed 11 November 2016.

Eurostat. (2015). *Statistics on Small and Medium-sized Enterprises—Dependent and Independent SMEs and Large Enterprises*. http://ec.europa.eu/eurostat/statistics-explained/index.php/Statistics_on_small_and_medium-sized_enterprises. Accessed 03 March 2018

Eurostat. (2017). *Cloud Computing Services*. http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises Accessed 08 April 2017.

Falk, R. F., & Miller, N. B. (1992). *A Primer for Soft Modeling*. University of Akron Press.

Featherman, M. F., & Pavlou, P. A. (2003). Predicting E-Services Adoption: A Perceived Risk Facets Perspective. *International Journal of Human-Computer Studies*, *59*(4), 451–474.

Feeny, D. F., & Willcocks, L. P. (1998). Core IS Capabilities for Exploiting Information Technology. *Sloan Management Review*, *9–21*.

Fenz, S., Ekelhart, A., & Neubauer, T. (2011). Information Security Risk Management: In Which Security Solutions Is It Worth Investing? *Communications of the Association for Information Systems*, *28*, 329–356.

Fiegenbaum, A., Hart, S., & Schendel, D. (1996). Strategic Reference Point Theory. *Strategic Management Journal*, *17*(2), 219–235.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision Support Approaches for Cyber Security Investment. *Decision Support Systems*, *86*, 13–23.

Finne, T. (1998). The Three Categories of Decision-Making and Information Security. *Computers & Security*, *17*(5), 397–405.

Fischer, F. (1998). Beyond Empiricism: Policy Inquiry in Post-Positivist Perspective. *Policy Studies Journal*, *26*(1), 129–146.

Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Addison-Wesley Pub. Co.

Fleischmann, M., Amirpur, M., Benlian, A., & Hess, T. (2014). *Cognitive Biases in Information Systems Research: A Scientometric Analysis*. Proceedings of the 22nd European Conference on Information Systems (ECIS), Tel Aviv, Israel.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(2), 407–429.

Fontana, A., & Frey, J. H. (2000). The Interview: From Structured Questions to Negotiated Text. In N. K. Denzin & Y. S. Lincoln (Eds.), *Handbook of Qualitative Research* (Vol. 2). Sage.

Forman, C. (2005). The Corporate Digital Divide: Determinants of Internet Adoption. *Management Science*, *51*(4), 641–654.

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, *18*(1), 39–50.

Forni, A. A., & van der Meulen, R. (2017). *Gartner Says Detection and Response is Top Security Priority for Organizations in 2017—Worldwide Spending on Information Security to Reach $90 Billion in 2017*.

Furby, L. (1978). Understanding the Psychology of Possession and Ownership. *Social Behavior and Personality*, *6*, 49–65.

Gal-Or, E., & Ghose, A. (2005). The Economic Incentives for Sharing Security Information. *Information Systems Research*, *16*(2), 186–208.

Gartner. (2016). *Gartner Says Worldwide Public Cloud Services Market Is Forecast to Reach $204 Billion in 2016*. https://www.gartner.com/en/newsroom/press-releases/2016-01-25-gartner-says-worldwide-public-cloud-services-market-is-forecast-to-reach-204-billion-in-2016 Accessed 11 April 2017.

Gartner, I. (2019). Digitization. In *Information Technology Gartner Glossary*. https://www.gartner.com/en/information-technology/glossary/digitization Accessed 21 March 2020.

Geletkanycz, M. A. (1997). The Salience of "Culture's Consequences": The Effects of Cultural Values on Top Executive Commitment to the Status Quo. *Strategic Management Journal*, *18*(8), 615–634.

Geletkanycz, M. A., & Black, S. S. (2001). Bound by the Past? Experience-Based effects on Commitment to the Strategic Status Quo. *Journal of Management*, *27*(1), 3–21.

Gerlach, J., Stock, R. M., & Buxmann, P. (2014). Never Forget Where You're Coming from: The Role of Existing Products in Adoptions of Substituting Technologies. *Journal of Product Innovation Management*, *31*(S1), 133–145.

Gewald, H., & Dibbern, J. (2009). Risks and Benefits of Business Process Outsourcing: A Study of Transaction Services in the German Banking Industry. *Information & Management*, *46*(4), 249–257.

Goes, P. B. (2013). Editor's Comments: Commonalities across IS Silos and Intradisciplinary Information Systems Research. *Management Information Systems Quarterly*, *37*(2), iii–vii.

Goffman, E. (1959). *The Presentation of Self in Everyday Life*. Penguin.

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services. *Journal of Management Information Systems*, *35*(1), 220–265.

Goodhue, D. L., & Straub, D. W. (1991). Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security. *Information & Management*, *20*(1), 13–27.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market Value of Involuntary Disclosures concerning Information Security. *MIS Quarterly*, *34*(3), 567–594.

Gordon, L. A., & Loeb, M. P. (2006). Economic Aspects of Information Security: An Emerging Field of Research. *Information Systems Frontiers*, *8*(5), 335–337.

Greenberg, A. (2019). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ Accessed 1 February 2019.

Greener, S. (2008). *Business Research Methods*. Ventus Publishing ApS.

Gregor, S. (2006). The Nature of Theory in Information Systems. *MIS Quarterly*, *30*(3), 611–642.

Grossklags, J., Christin, N., & Chuang, J. (2008). *Security Investment (Failures) in Five Economic Environments: A Comparison of Homogeneous and Heterogeneous User Agents*. Proceedings of the 7th Workshop on the Economics of Information Security, London, United Kingdom.

Guarro, S. B. (1987). Principles and Procedures of the LRAM Approach to Information Systems Risk Analysis and Management. *Computers & Security*, *6*(6), 493–504.

Guba, E. G., & Lincoln, Y. S. (1994). Competing Paradigms in Qualitative Research. In N. V. ; L. Denzin (Ed.), *Handbook of Qualitative Research* (Vol. 2, pp. 163–194). Sage.

Gupta, M., Rees, J., Chaturvedi, A., & Chi, J. (2006). Matching Information Security Vulnerabilities to Organizational Security Profiles: A Genetic Algorithm Approach. *Decision Support Systems*, *41*(3), 592–603.

Gurbaxani, V., & Whang, S. (1991). The Impact of Information Systems on Organizations and Markets. *Communications of the ACM*, *34*(1), 59–73.

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2013). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)* (2nd ed.). Sage Publications.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–152.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An Assessment of the Use of Partial Least Squares Structural Equation Modeling in Marketing Research. *Journal of the Academy of Marketing Science*, *40*(3), 414–433.

Halbrecht, H. (1977). Interview with: William Dougherty, President and Director, North Carolina National Bank Corporation. *MIS Quarterly*, *1*(1), 1–6.

Hansen, J. V., Lowry P. B, Meservy R., & McDonald, D. M. (2007). Genetic Programming for Prevention of Cyberterrorism through Dynamic and Evolving Intrusion Detection. *Decision Support Systems*, *43*(3), 1362–1374.

Herath, H. S. B., & Herath, T. C. (2008). Investments in Information Security: A Real Options Perspective with Bayesian Postaudit. *Journal of Management Information Systems*, *25*(3), 337–375.

Herath, T., & Rao, H. R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems*, *18*(2), 106–125.

Hermanns, H. (2004). Interviewing as an Activity. In U. Flick, E. von Kardoff, & I. Steinke (Eds.), *A Companion to Qualitative Research* (pp. 209–213). Sage.

Hess, T., Matt, C., Benlian, A., & Wiesböck, F. (2016). Options for Formulating a Digital Transformation Strategy. *MIS Quarterly Executive*, *15*, 123–139.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *Management Information Systems Quarterly*, *28*(1), 7–705.

Hintsch, J., & Turowski, K. (2019). Enterprise Computing: A Case Study on Current Practices in SAP Operations. *International Conference on Business Information Systems*, 124–135.

Hovorka, D. S., & Lee, A. S. (2010). Reframing Interpretivism and Positivism as Understanding and Explanation: Consequences for Information Systems Research. *Proceedings of the 31st International Conference on Information Systems*, Saint Louis, USA.

Howorth, C. A. (2001). Small Firms' Demand for Finance: A Research Note. *International Small Business Journal*, *19*(4), 78–86.

Hsieh, H. F., & Shannon, S. E. (2005). Three Approaches to Qualitative Content Analysis. *Qualitative Health Research*, *15*(9), 1277–1288.

Hsu, C., Lee, J.-N., & Straub, D. W. (2012). Institutional Influences on Information Systems Security Innovations. *Information Systems Research*, *23*(3), 918–939.

Hsu, C. S., Chou, S.-W., & Min, H.-T. (2015). *Understanding Clients' Intentions to Explore Software-as-a-Service (SaaS) Features: A Social Capital Theory Perspective*. Proceedings of the 19th Pacific Asia Conference on Information Systems (PACIS).

Hsu, C. W. (2009). Frame Misalignment. Interpreting the Implementation of Information Systems Security Certification in an Organization. *European Journal of Information Systems*, *18*(2), 140–150.

Hu, L.-T., & Bentler, P. M. (1998). Fit Indices in Covariance Structure Modeling: Sensitivity to Underparameterized Model Misspecification. *Psychological Methods*, *3*(4), 424–453.

Hu, Q., Hart, P., & Cooke, D. (2007). The Role of External and Internal Influences on Information Systems Security – A Neo-Institutional Perspective. *Journal of Strategic Information Systems*, *16*(2), 153–172.

Huang, C. D., Behara, R. S., & Goo, J. (2014). Optimal Information Security Investment in a Healthcare Information Exchange: An Economic Analysis. *Decision Support Systems*, *61*, 1–11.

Huber, G. P. (1980). *Managerial Decision Making*. Scott Foresman & Co, Glenview, USA.

Huber, G. P. (1981). The Nature of Organizational Decision-Making and the Design of Decision Support Systems. *Management Information Systems Quarterly*, *5*(2), 1–10.

Hui, K.-L., Hui, W., & Yue, W. T. (2012). Information Security Outsourcing with System Interdependency and Mandatory Security Requirement. *Journal of Management Information Systems*, *29*(3), 117–156.

Hulland, J. (1999). Use of Partial Least Squares (PLS) in Strategic Management Research: A Review of Four Recent Studies. *Strategic Management Journal*, *20*(2), 195–204.

Iacovou, C. L., Benbasat, I., & Dexter, A. S. (1995). Electronic Data Interchange and Small Organizations: Adoption and Impact of Technology. *MIS Quarterly*, *19*(4), 465–485.

Iannacci, F., Fearon, C., & Pole, K. (2020). From Acceptance to Adaptive Acceptance of Social Media Policy Change: A Set-Theoretic Analysis of B2B SMEs. Information Systems Frontiers, 1-18. *Information Systems Frontiers*, 1–18.

IBM. (2012). *The Flood of Big Data—Driving Marketing Effectiveness by Managing* [Infographic]. https://www.ibmbigdatahub.com/infographic/flood-big-data Accessed 08 august 2018.

IDC. (2014). *IDC 50th Anniversary—Transformation Everywhere*. https://issuu.com/internationaldatacorp/docs/idc50thanniversary_ebook_final Accessed 14 April 2017.

IDC. (2016). *Worldwide Public Cloud Services Spending Forecast to Double by 2019, According to IDC*. https://www.idc.com/getdoc.jsp?containerId=prUS45340719 Accessed 11 November 2016.

ISO. (2018). *ISO/IEC 27000:2018(E): Information technology—Security techniques—Information Security Management Systems—Overview and Vocabulary*. International Organization for Standardization, Geneva, Switzerland. https://standards.iso.org/ittf/PubliclyAvailableStandards/

Jaeger, L., Ament, C., & Eckhardt, A. (2017). *The Closer You Get the More Aware You Become–A Case Study about Psychological Distance to Information Security Incidents*. Proceedings of the 38th International Conference on Information Systems.

James, H. S. (1999). Owner as Manager, Extended Horizons and the Family Firm. *International Journal of the Economics of Business*, *6*(1), 41–55.

Jeong, C. Y., Lee, S.-Y. T., & Lim, J.-H. (2019). Information Security Breaches and IT Security Investments: Impacts on Competitors. *Information & Management*, *56*(5), 681–695.

Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly*, *34*(3), 549–566.

Kahneman, D., Knetsch, J. L., & Thaler, R. H. (1991). Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias. *The Journal of Economic Perspectives*, *5*(1), 193–206.

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, *47*(2), 263–291.

Kahneman, D., & Tversky, A. (1984). Choices, Values, and Frames. *American Psychologist*, *39*(4), 341.

Kam, H. J., Mattson, T., & Goel, S. (2019). A Cross Industry Study of Institutional Pressures on Organizational Effort to Raise Information Security Awareness. *Information Systems Frontiers*, 1–24.

Kaplan, B., & Maxwell, J. A. (1994). Evaluating Health Care Information Systems: Methods and Applications. In J. G. Anderson, C. E. Ayden, & S. J. Jay (Eds.), *Qualitative Research Methods for Evaluating Computer Information Systems*. Sage.

Kaplan, B., & Maxwell, J. A. (2005). Qualitative Research Methods for Evaluating Computer Information Systems. In *Evaluating the Organizational Impact of Healthcare Information Systems* (pp. 30–55). Springer.

Kaspersky. (2017). New Threats, New Mindset: Being Risk Ready in a World of Complex Attacks. *How to Address Incident Response Challenges*. https://www.kaspersky.com/blog/incident-response-report/

Keen, P. G. W. (1980). MIS Research: Reference Disciplines and a Cumulative Tradition. *First International Conference on Information Systems (ICIS)*, 9–18.

Kehr, F., & Kowatsch, T. (2015). *Quantitative Longitudinal Research: A Review of IS Literature, and a Set of Methodological Guidelines*. Proceedings of the 23rd European Conference on Information Sytems (ECIS), Münster, Germany.

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information Security Threats and Practices in Small Businesses, Information Systems Management. *Information Systems Management*, *22*(2), 7–19.

Kets De Vries, M. F. R. (1995). *Organizational Paradoxes: Clinical Approaches to Management* (Vol. 2). Routledge.

Khansa, L., & Liginlal, D. (2009). Quantifying the Benefits of Investing in Information Security. *Communications of the ACM*, *52*(11), 113–117.

Kim, H.-W., & Kankanhalli, A. (2009). Investigating User Resistance to Information Systems Implementation: A Status Quo Bias Perspective. *MIS Quarterly*, *33*(3), 567–582.

Kim, S., & Lee, H. J. (2007). A Study on Decision Consolidation Methods using Analytic Models for Security Systems. *Computers & Security*, *26*(2), 145–153.

Klein, G. A. (2017). *Sources of Power: How People make Decisions* (20th Anniversary). MIT Press.

Klein, H. K., & Myers, M. D. (1999). A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. *MIS Quarterly*, *23*(1), 67–93.

Klesel, M., Ndicu, M., & Niehaves, B. (2016). *Exploring Psychological Ownership of IT: An Empirical Study*. Proceedings of the 24th European Conference on Information Systems (ECIS), Istanbul, Turkey.

Kolfal, B., Patterson, R. A., & Yeo, M. L. (2013). Market Impact on IT Security Spending. *Decision Sciences*, *44*(3), 517–556.

Kotulic, A., & Clark, J. G. (2004). Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. Information & Management, 41(5). *Information & Management*, *41*(5), 597–607.

Kraft, P., Rise, J., Sutton, S., & Røysamb, E. (2005). Perceived Difficulty in the Theory of Planned Behaviour: Perceived Behavioural Control or Affective Attitude? *British Journal of Social Psychology*, *44*(3), 479–496.

Kumar, R. L., Park, S., & Subramaniam, C. (2008). Understanding the Value of Countermeasure Portfolios in Information Systems Security. *Journal of Management Information Systems*, *25*(2), 241–279.

Kwok, L., & Longley, D. (1999). Information Security Management and Modelling. *Information Management & Computer Security*, *7*(1), 30–40.

Kwon, J., & Johnson, M. E. (2014). Proactive Versus Reactive Security Investments in the Healthcare Sector. *Management Information Systems Quarterly*, *38*(2), 451–471.

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. (2014). Information Security Awareness and Behavior: A Theory-based Literature Review. *Management Research Review*, *37*(12), 1049–1092.

Lee, A. S. (1999). *Research MIS*. Oxford University Press.

Lee, C. H., Geng, X., & Raghunathan, S. (2013). Contracting Information Security in the Presence of Double Moral Hazard. *Information Systems Research*, *24*(2), 295–311.

Lee, M.-C. (2009). Factors Influencing the Adoption of Internet Banking: An Integration of TAM and TPB with Perceived Risk and Perceived Benefits. *Electronic Commerce Reserach and Applications*, *8*(3), 130–141.

Lee, S.-G., & Chae, S. H. C. (2013). Drivers and Inhibitors of SaaS Adoption in Korea. *International Journal of Information Management*, *33*(3), 429–440.

Lee, Y., & Chen, A. N. K. (2011). Usability Design and Psychological Ownership of a Virtual World. *Journal of Management Information Systems*, *28*(3), 269–307.

Lee, Y. J., Kauffman, R. J., & Sougstad, R. (2011). Profit-Maximizing Firm Investments in Customer Information Security. *Decision Support Systems*, *51*(4), 904–920.

Lee, Y., & Larsen, K. R. (2009). Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-Malware Software. *European Journal of Information Systems*, *18*(2), 177–187.

Leimeister, S., Böhm, M., Riedl, C., & Krcmar, H. (2010). *The Business Perspective of Cloud Computing: Actors, Roles and Value Networks*. Proceedings of the 18th European Conference on Information Systems (ECIS), Pretoria, South Africa.

Lemos, R. (2017). *Recent Ransomware Attacks: Is it an Epidemic or Overblown?* https://searchsecurity.techtarget.com/feature/Recent-ransomware-attacks-Is-it-an-epidemic-or-overblown

Levy, J. S. (1992). An Introduction to Prospect Theory. *Political Psychology*, *13*(2), 171–186.

Levy, J. S. (1997). Prospect Theory, Rational Choice, and International Relations. *International Studies Quarterly*, *41*(1), 87–112.

Levy, Y., & Ellis, T. J. (2006). A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. *Informing Science*, *9*, 181–212.

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, *11*(7), 394–413.

Lin, A., & Chen, N.-C. (2012). Cloud Computing as an Innovation: Percepetion, Attitude, and Adoption. *International Journal of Information Management*, *32*(6), 533–540.

Lindell, M. K., & Whitney, D. J. (2001). Accounting for Common Method Variance in Cross-sectional Research Designs. *Journal of Applied Psychology*, *86*(1), 114–121.

Liu, D., Ji, Y., & Mookerjee, V. (2011). Knowledge Sharing and Investment Decisions in Information Security. *Decision Support Systems*, *52*(1), 95–107.

Loske, A., Widjaja, T., Benlian, A., & Buxmann, P. (2014). *Perceived IT Security Risks in Cloud Adoption: The Role of Perceptual Incongruence Between Users and Providers*. Proceedings of the 22nd European Conference on Information Systems.

Lowry, P. B., Moody, G. D., Gaskin, J., Galletta, D. F., Humpherys, S. L., Barlow, J. B., & Wilson, D. W. (2013). Evaluation Journal Quality and the Association for Infromatio

Sytems Senior Scholars' Journal Basket via Bibliometric Measures: Do Expert Journal Assessments Add Value? *MIS Quarterly*, *37*(4), 993–1012.

Lowry, P. B., Romans, D., & Curtis, A. (2004). Global Journal Prestige and Supporting Disciplines: A Scientometric Study of Information Systems Journals. *Journal of the Association for Information Systems*, *5*(2), 29–80.

Lowry, Paul B., Dinev, T., & Willison, R. (2017). Why Security and Privacy Research Lies at the Centre of the Information Systems (IS) Artefact: Proposing a Bold Research Agenda. *European Journal of Information Systems*, *26*(6), 546–563.

Lumpkin, G. T., & Brigham, K. H. (2011). Long-Term Orientation and Intertemporal Choice in Family Firms. *Entrepreneurship Theory and Practice*, *35*(6), 1149–1169.

MacGregor, R. C. (2003). Strategic Alliance and Perceived Barriers to Electronic Commerce Adoption in SMEs. *Journal of Systems and Information Technology*, *7*(1), 27–47.

MacGregor, R. C., & Vrazalic, L. (2005). A Basic Model of Electronic Commerce Adoption Barriers: A Study of Regional Small Businesses in Sweden and Australia. *Journal of Small Business and Enterprise Development*, *12*(4), 510–527.

Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does Sample Size matter in Qualitative Research? A Review of Qualitative Interviews in IS Research. *Journal of Computer Information Systems*, *54*(1), 11–22.

Mathias, B. D., & Williams, D. W. (2014). The Impact of Role Identities on Entrepreneurs' Evaluation and Selection of Opportunities. *Journal of Management*, *43*(3), 892–918.

Mattia, A., & Dhillon, G. (2003). *Applying Double Loop Learning to Interpret Implications for Information Systems Security Design*. *3*, 2521–2526.

Mayadunne, S., & Park, S. (2016). An Economic Model to Evaluate Information Security Investment of Risk-taking Small and Medium Enterprises. *International Journal of Production Economics*, *182*, 519–530.

Mayer, P., Kunz, A., & Volkamer, M. (2017). *Reliable Behavioural Factors in the Information Security Context*. Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy.

Mayring, P. (2014). *Qualitative Content Analysis: Theoretical Foundation, Basic Procedures and Software Solution*. Social Science Open Access Repository, Klagenfurt, Germany

Mc Farlan, Warren. (2016). *Keynote CTO Forum Warren McFarlan—Technology Changes the Way You Compete*. https://www.youtube.com/watch?v=ao_7IePryoM Accessed 19 December 2019.

McLellan, C. (2016). *SaaS in 2016: The Key Trends*. CLOUD - How to Do SaaS Right. https://www.zdnet.com/article/saas-in-2016-the-key-trends/ Accessed 14 April 2017.

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing*. *SP 800–145*. https://csrc.nist.gov/publications/detail/sp/800-145/final Accessed 28 March 2020.

Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Information Technology and Organizational Performance: An Integrative Model of IT Business Value. *MIS Quarterly*, *28*(2), 283–322.

Menard, P., Warkentin, M., & Lowry, P. B. (2018). The Impact of Collectivism and Psychological Ownership on Protection Motivation: A Cross-Cultural Examination. *Computers & Security*, *75*, 147–166.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative Data Analysis: An Expanded Sourcebook*. Sage.

Miles, M. B., Huberman, A. M., & Saldana, J. (2013). *Qualitative Data Analysis. A Methods Sourcebook* (Vol. 3). Sage.

Miller, S., Wagner, C., Aickelin, U., & Garibaldi, J. M. (2016). Modelling Cyber-Security Experts' Decision Making Processes using Aggregation Operators. *Computers & Security*, *62*, 229–245.

Milne, S., Orbell, S., & Sheeran, P. (2002). Combining Motivational and Volitional Interventions to Promote Exercise Participation: Protection Motivation Theory and Implementation Intentions. *British Journal of Health Psychology*, *7*(2), 163–184.

Milovich, M. (2019). From Technology Revolution to Digital Revolution: An Interview with F. Warren McFarlan from the Harvard Business School. , 44(1), pp-pp. *Communications of the Association for Information Systems*, *44*(1), 152–167.

Mintzberg, H. (1989). The Structuring of Organizations. In *Readings in Strategic Management* (pp. 322–352). Palgrave.

MIS Quarterly. (2019). Editorial Mission Statement. https://misq.org/mission Accessed 19 December 2019.

Moore, S., & Keen, E. (2019). *Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019: Detection, Response and Privacy Driving Demand for Security Products and Services*. In Gartner (Ed.). https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019. Accessed 29 January 2019

Moqbel, M. A., & Bartelt, V. L. (2015). Consumer Acceptance of Personal Cloud: Integrating Trust and Risk with the Technology Acceptance Model. *AIS Transactions on Replication Research*, *1*(1), 1–5.

Morakanyane, R., Grace, A. A., & O'Reilly, P. (2017). Conceptualizing Digital Transformation in Business Organizations: A Systematic Review of Literature. *Bled EConference Proceedings*, 427–444.

Morse, J. M. (1994). *Designing Funded Qualitative Research*. Sage.

Mou, J., Cohen, J., & Kim, J. (2017). *A Meta-Analytic Structural Equation Modeling Test of Protection Motivation Theory in Information Security Literature.* Proceedings of the 38th International Conference on Information Systems (ICIS), Seoul, South Korea.

Muehe, S., & Drechsler, A. (2017). Towards a Framework to Improve IT Security and IT Risk Management in Small and Medium Enterprises. *International Journal of Systems and Society*, *3*(2), 44–56.

Müller, S. D., Holm, S. R., & Søndergaard, J. (2015). Benefits of Cloud Computing: Literature Review in a Maturity Model Perspective. *Communications of the Association for Information Systems*, *37*(1), 851 – 878.

Myers, M. D. (1997). Qualitative Research in Information Systems. *MIS Quarterly*, *21*(2), 241–242.

Nazareth, D. L., & Choi, J. (2015). A System Dynamics Model for Information Security Management. *Information & Management*, *52*(1), 123–134.

Newton, J. (1985). Strategies for Problem Prevention. *IBM Systems Journal*, *24*(3/4), 248–263.

Ng, B. Y., & Feng, A. E. (2006). *An Exploratory Study on Managerial Security Concerns in Technology Start-ups*. Proceedings of Pacific Asia Conference on Information Systems, Chiayi, Taiwan.

Nunnally, J. C. (1978). *Psychometric Theory* (Vol. 2). McGraw-Hill.

OECD. (1997). *Small Businesses, Job Creation and Growth: Facts, Obstacles and Best Practices*. Organisation for Economic Co-operation and Development. https://www.oecd.org/cfe/smes/2090740.pdf

OECD. (2005). *Glossary of Statistical Terms—Small and Medium-sized Enterprises (SMEs)*. https://stats.oecd.org/glossary/detail.asp?ID=3123

OECD. (2016). *Financing SMEs and Entrepreneurs 2016: An OECD Scoreboard*. Definition of SMEs in China. https://www.oecd-ilibrary.org/industry-and-services/financing-smes-and-entrepreneurs-2016_fin_sme_ent-2016-en

OECD. (2017). *Small, Medium, Strong. Trends in SME Performance and Business Conditions*. https://www.oecd.org/industry/small-medium-strong-trends-in-sme-performance-and-business-conditions-9789264275683-en.htm

Okoli, J. C., & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. *Sprouts: Working Papers on Information Systems, 10*(26), 1–46.

Olt, C., Gerlach, J., Sonnenschein, R., & Buxmann, P. (2019). *On the Benefits of Senior Executives' Information Security Awareness.* Proceedings of the 40th International Conference on Information Systems (ICIS), Munich, Germany.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying Information Technology in Organizations: Research Approaches and Assumptions. *Information Systems Research*, *2*(1), 1–28.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' Behavior towards IS Security Policy Compliance*. Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS), Hawaii, US.

Paré, G., Trudel, M. C., Jaana, M., & Kitsiou, S. (2015). Synthesizing Information Systems Knowledge: A Typology of Literature Reviews. *Information & Management*, *52*(2), 183–199.

Paulsen, C., & Byers, R. (2019). NISTIR 7298 Revision 3 Glossary of Key Information Security Terms. In *I National Institute of Standards and Technology Interagency or Internal Report 7298 Revision 3*. https://csrc.nist.gov/glossary

Pearlson, K., & Saunders, C. S. (2007). *Managing and Using Information Systems: A Strategic Approach* (4th ed.). John Wiley and Sons.

Pierce, J. L., Kostova, T., & Dirks, K. T. (2001). Toward a Theory of Psychological Ownership in Organizations. *Academy of Management Review*, *26*(2), 298–310.

Pierce, J. L., Kostova, T., & Dirks, K. T. (2003). The State of Psychological Ownership: Integrating and Extending a Century of Research. *Review of General Psychology*, *7*(1), 84–107.

Piscitello, L., & Sgobbi, F. (2004). Globalisation, E-Business and SMEs: Evidence from the Italian District of Prato. *Small Business Economics*, *22*(5), 333–347.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y. Y., & Podsakoff, N. P. (2003). Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology*, *88*(5), 879–903.

Polites, G. L., & Karahanna, E. (2012). Shackled to the Status Quo: The Inhibiting Effects of Incumbent System Habit, Switching Costs, and Inertia on New System Acceptance. *MIS Quarterly*, *36*(1), 21–42.

Preacher, K. J., & Hayes, A. F. (2008). Asymptotic and Resampling Strategies For Assessing and Comparing Indirect Effects in Multiple Mediator Models. *Behavior Research Methods*, *40*(3), 879–891.

Purser, S. A. (2004). Improving the ROI of the Security Management Process. *Computers & Security*, *23*(7), 542–546.

Qian, Y., Fang, Y., & Gonzalez, J. J. (2012). Managing Information Security Risks During New Technology Adoption. *Computers & Security*, *31*(8), 859–869.

Ravitch, S. M., & Riggan, M. (2016). *Reason & Rigor: How Conceptual Frameworks Guide Research* (Vol. 2). SAGE.

Rees, L. P., Deane, J. K., Rakes, T. R., & Baker, W. H. (2011). Decision Support for Cybersecurity Risk Planning. *Decision Support Systems*, *51*(3), 493–505.

Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic Optimism on Information Security Management. *Computers & Security*, *31*, 221–232.

Riemenschneider, C. K., Harrison, D. A., & Mykytyn Jr, P. P. (2003). Understanding IT Adoption Decisions in Small Business: Integrating Current Theories. *Information & Management*, *40*(4), 269–285.

Rivard, S. (2014). Editor's Comments: The Ions of Theory Construction. *MIS Quarterly*, *38*(2), iii–xiv.

Rivera, J., & van der Meulen, R. (2014). Gartner Survey Reveals That SaaS Deployments Are Now Mission Critical. *Survey Reveals Enterprise Cloud Adoption Plans Through 2017*. Accessed 11 November 2016.

Rogers, R. (1983). Cognitive and Physiological Processes in Fear-based Attitude Change: A Revised Theory of Protection Motivation. In Cacioppo J & R. Petty (Eds.), *Social Psychophysiology: A Sourcebook* (pp. 153–176). Guilford Press.

Roodhooft, F., & Warlop, L. (1999). On the Role of Sunk Costs and Asset Specificity in Outsourcing Decisions: A Research Note. *Accounting, Organizations and Society*, *24*(4), 363–369.

Roster, C. A., & Richins, M. L. (2009). Ambivalence and Attitudes in Consumer Replacement Decisions. *Journal of Consumer Psychology*, *19*(1), 48–61.

Rudmin, F. W., & Berry, J. W. (1987). Semantics of Ownership: A Free-recall Study of Property. *Psychological Record*, *37*, 257–268.

Ryan, J. J. C. H., & Ryan, D. J. (2006). Expected Benefits of Information Security Investments. *Computers & Security*, *25*(8), 579–588.

Salavou, H., Baltas, G., & Lioukas, S. (2004). Organisational Innovation in SMEs: The Importance of Strategic Orientation and Competitive Structure. *European Journal of Marketing*, *38*(9/10), 1091–1112.

Saldaña, J. (2009). *The Coding Manual for Qualitative Researchers*. Sage.

Salge, T.-O., Kohli, R., & Barrett, M. (2015). Investing in Information Systems: On the Behavioral and Institutional Search Mechanisms Underpinning Hospitals' IS Investment Decisions. *Management Information Systems Quarterly*, *39*(1), 61–89.

Samuelson, W., & Zeckhauser, R. (1988). Status Quo Bias in Decision Making. *Journal of Risk and Uncertainty*, *1*(1), 7–59.

Sarker, S., Xiao, X., & Beaulieu, T. (2013). Qualitative Studies in Information Systems: A Critical Review and some Guiding Principles. *MIS Quarterly*, *37*(4), iii–xviii.

Sarstedt, M., Henseler, J., & Ringle, C. M. (2011). Multigroup Analysis in Partial Least Squares (PLS) Path Modeling: Alternative Methods and Empirical Results. In M. Sarstedt, M. Schwaiger, & C. R. Taylor (Eds.), *Measurement and Research Methods in International Marketing (Advances in International Marketing)* (Vol. 22, pp. 195–218). Emerald Group Publishing Limited.

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2007). *Research Methods for Business Students* (4th ed.). Financial Times Prentice Hall.

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2015). *Research Methods for Business Students* (Vol. 7). Pearson Education.

Sawik, T. (2013). Selection of Optimal Countermeasure Portfolio in IT Security Planning. *Decision Support Systems*, *55*(1), 156–164.

Schatz, D., & Bashroush, R. (2017). Economic Valuation for Information Security Investment: A Systematic Literature Review. *Information Systems Frontiers*, *19*(5), 1205–1228.

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. John Wiley and Sons.

Schweitzer, M. (1995). Multiple Reference Points, Framing, and the Status Quo Bias in Health Care Financing Decisions. *Organizational Behavior and Human Decision Processes*, *63*(1), 69–72.

Schwenk, C. (1984). Cognitive Simplification Processes in Strategic Decision-Making: Insights from Behavioral Decision Theory and Cognitive Psychology. *Strategic Management Journal*, *5*(2), 111–128.

Sen, R., & Borle, S. (2015). Estimating the Contextual Risk of Data Breach. An Empirical Approach. *Journal of Management Information Systems*, *32*(2), 314–341.

Shoham, A., & Fiegenbaum, A. (2002). Competitive Determinants of Organizational Risk-Taking Attitude: The Role of Strategic Reference Points. *Management Decision*, *40*(2), 127–141.

Simon, H. A. (1959). Theories of Decision-Making in Economics and Behavioral Science. *The American Economic Review*, *49*(3), 253–283.

Simon, H. A. (1960). *The Ford Distinguished Lectures: Vol. 3. The New Science of Management Decision*. Harper & Brothers.

Simon, H. A. (1979). Rational Decision Making in Business Organisations. *The American Economic Review*, *69*(4), 493–513.

Simon, H. A. (1997). *Administrative Behavior—A Study of Decision Making Processes in Administrative Organizations* (4th ed.). The Free Press.

Sinha, T. (1994). Prospect Theory and the Risk Return Association: Another Look. *Journal of Economic Behavior & Organization*, *24*(2), 225–231.

Siponen, M. (2005). An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice. *European Journal of Information Systems*, *14*(3), 303–315.

Slovic, P. (1975). Choice Between Equally-Valued Alternatives. *Journal of Experimental Psychology*, *1*(3), 280–287.

Sonnenschein, R., Loske, A., & Buxmann, P. (2017). *The Role of Top Managers' IT Security Awareness in Organizational IT Security Management*. Proceedings of the 38th International Conference on Information Systems, South Korea.

Spears, J. L., & Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS Quarterly*, *34*(3), 503–522.

Stockdale, R., & Standing, C. (2006). A Classification Model to Support SME E-Commerce Adoption Initiatives. *Journal of Small Business and Enterprise Development*, *13*(3), 381–394.

Straub, D. W., & Welke, R. J. (1998). Coping with Systems Risk. Security Planning Models for Management Decision Making. *MIS Quarterly*, *22*(4), 441–469.

Straub, Detmar W. (1990). Effective IS Security. An Empirical Study. *Information Systems Research*, *1*(3), 255–276.

Sun, L., Srivastava, R. P., & Mock, T. J. (2006). An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief Functions. *Journal of Management Information Systems, 22*(4), 109–142.

Synergy. (2016). *2015 Review Shows $110 Billion Cloud Market Growing at 28% Annually*. https://www.srgresearch.com/articles/2015-review-shows-110-billion-cloud-market-growing-28-annually Accessed 11 November 2016.

Teo, T. L., Chan, C., & Parker, C. (2004). *Factors Affecting e-Commerce Adoption by SMEs: A Meta-Analysis*. In Proceedings of the 15th Australasian Conference on Information Systems, 54–64.

Thong, J. Y. L. (1999). An Integrated Model of Information Systems Adoption in Small Businesses. *Journal of Management Information Systems, 15*(4), 187–214.

Thong, J. Y. L. (2001). Resource Constraints and Information Systems Implementation in Singaporean Small Businesses. *The International Journal of Management Science, 29*(2), 143–156.

Thong, J. Y. L., & Yap, C. S. (1995). CEO Characteristics, Organizational Characteristics and Information Technology Adoption in Small Businesses. *Omega International Journal of Management Science, 23*(4), 429–442.

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the Role of Cognitive and Cultural Biases in the Internalization of Information Security Policies: Recommendations for Information Security Awareness Programs. *Computers & Security, 52*, 128–141.

Tversky, A., & Kahneman, D. (1975). Judgment under Uncertainty: Heuristics and Biases. In D. Wendt & C. Vlek (Eds.), *Utility, Probability, and Human Decision Making* (pp. 141–162). Springer Netherlands.

Tversky, A., & Kahneman, D. (1985). The Framing of Decisions and the Psychology of Choice. In V. T. Covello, J. L. Mumpower, P. J. M. Stallen, & V. R. R. Uppuluri (Eds.), *Environmental Impact Assessment, Technology Assessment, and Risk Analysis* (pp. 107–129). Springer-Verlag Berlin Heidelberg.

United Nations. (2008). *International Standard Industrial Classification of All Economic Activities, Rev.4*. https://unstats.un.org/unsd/publication/seriesm/seriesm_4rev4e.pdf

United States Business Administration. (2018). *US Small Business Profile. Office of Advocacy*. https://www.sba.gov/sites/default/files/advocacy/2018-Small-Business-Profiles-US.pdf Accessed 8 January 2019.

Urquhart, J. (2008). *The Great Paradigm Shift of Cloud Computing is Not Self-service.* Cnet. https://www.cnet.com/news/the-great-paradigm-shift-of-cloud-computing-is-not-self-service/ Accessed 22 December 2019.

Van de Ven, A. H. (2007). *Engaged Scholarship: A Guide for Organizational and Social Research*. Oxford University Press.

van der Meulen, R., & Rivera, J. (2015). Gartner Says Cloud Is a Viable Option, But Not a Top Consideration for Many CIOs. *I&O Leaders Should Institute a "Cloud-First" Consideration for Every Project on an Application-by-Application Basis*. Accessed 10 November 2016.

Van Dyne, L., & Pierce, J. L. (2004). Psychological Ownership and Feelings of Possession: Three Field Studies Predicting Employee Attitudes and Organizational Citizenship Behavior. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior*, *25*(4), 439–459.

Van Niekerk, J. F., & Von Solms, R. (2010). Information Security Culture: A Management Perspective. *Computers & Security*, *29*(4), 476–486.

Vandewalle, D., Van Dyne, L., & Kostova, T. (1995). Psychological Ownership: An Empirical Examination of its Consequences. *Group & Organization Management*, *20*(2), 210–226.

Veit, D., Clemons, E., Benlian, A., Buxmann, P., Hess, T., Kundisch, D., Leimeister, J. M., Spann, M., & Loos, P. (2014). Business Models—An Information Systems Research Agenda. In: *Software Business & Information Systems Engineering - Research Note*, *1*, 45–53.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3).

Venkatraman, N. (1994). IT-enabled Business Transformation: From Automation to Business Scope Redefinition. *Sloan Management Review*, *35*(2), 73–87.

Verhees, F. J., & Meulenberg, M. T. (2004). Market Orientation, Innovativeness, Product Innovation, and Performance in Small Firms. *Journal of Small Business Management*, *42*(2), 134–154.

Verizon. (2018). *Verizon Data Breach Investigations Report*. https://enterprise.verizon.com/resources/reports/dbir/ Accessed 08 August 2018.

Vetter, J., Benlian, A., & Hess, T. (2011). *Setting Targets Right! How Non-Rational Biases Affect the Risk Preference of IT-Outsourcing Decision-makers—An Empirical Investigation.* Proceedings of 19th the European Conference of Information Systems (ECIS), Helsinki, Finland.

vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., & Cleven, A. (2009). *Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process*. In Proceedings of the 17th European Conference on Information Systems 2009, Verona, Italy.

von Solms, R., Vandehaar, H., von Solms, S. H., & Caelli, W. J. (1994). A Framework for Information Security Evaluation. *Information & Management*, *26*(3), 143–153.

Vroom, V. H., & Yetton, P. W. (1973). *Leadership and Decision-Making*. University of Pittsburgh Press.

Wang, J., Chaudhury, A., & Rao, H. R. (2008). A Value-at-Risk Approach to Information Security Investment. *Information Systems Research*, *19*(1), 106–120.

Wang, T., Kannan, K. N., & Rees Ulmer, J. (2013). The Association Between the Disclosure and the Realization of Information Security Risk Factors. *Information Systems Research*, *24*(2), 201–218.

We Are Social Ltd. (2018). *Global Digital Population as of July 2018* [Infographic]. In Statista. https://wearesocial.com/blog/2018/01/global-digital-report-2018 Accessed 08 August 2018.

Webb, T. L., & Sheeran, P. (2006). Does Changing Behavioral Intentions Engender Behavior Change? A Meta-Analysis of the Experimental Evidence. *Psychological Bulletin*, *132*(2), 249–268.

Weber, R. (2004). Editor's Comments: The Rhethoric of Positivism vs. Interpretivism: A Personal View. *MIS Quarterly*, *28*(1), iii–xii.

Webster, J., & Watson, R. T. (2002). Analyzing The Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), xiii–xxiii.

Weishäupl, E., Yasasin, E., & Schryen, G. (2015). *A Multi-Theoretical Literature Review on Information Security Investments using the Resource-Based View and the Organizational Learning Theory*. Proceedings of the 36th International Conference on Information Systems (ICIS), Fort Worth, USA.

Weishäupl, E., Yasasin, E., & Schryen, G. (2018). Information Security Investments: An Exploratory Multiple Case Study on Decision-Making, Evaluation and Learning. *Computers & Security*, *77*.

Welsh, J. A., & White, J. F. (1981). A Small Business is not a Little Big Business. *Harvard Business Review*, *59*(4), 18–32.

West, G. M. (1975). MIS in Small Companies. *Journal of Systems Management*, *26*(4), 10–13.

Wielicki, T., & Arendt, L. (2010). A Knowledge-driven Shift in Perception of ICT Implementation Barriers: Comparative Study of US and European SMEs. *Journal of Information Science*, *36*(2), 162–174.

Willison, R., & Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly*, *37*(1), 1–20.

Witte, K. (1996). Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale. *Journal of Health Communication*, *1*(4), 317–342.

Wolcott, H. F. (1994). *Transforming Qualitative Data: Description, Analysis, and Interpretation*. Sage.

Wolff, J. (2016). Perverse Effects in Defense of Computer Systems. When More Is Less. *Journal of Management Information Systems*, *33*(2), 597–620.

Wolfswinkel, J., Furtmueller, E., & Wilderom, C. (2013). Using Grounded Theory as a Method for Rigorously Reviewing Literature. *European Journal of Information Systems*, *22*(1), 45–55.

Wood, C. C. (1988). A Context for Information Systems Security Planning. *Computers & Security*, *7*(5), 455–465.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test. *Computers in Human Behavior*, *24*(6), 2799–2816.

World Economic Forum. (2010). *Exploring the Future of Cloud Computing: Riding the Next Wave of Technology-driven Transformation*. https://www.weforum.org/reports/exploring-future-cloud-computing-riding-next-wave-technology-driven-transformation Accessed 13 April 2017.

World Economic Forum. (2019). *The Global Risks Report 2019*. https://www.weforum.org/reports/the-global-risks-report-2019 Accessed 14 February 2019.

Worrall, L., Levy, M., & Powell, P. (2005). Strategic Intent and E-Business in SMEs: Enablers and Inhibitors. *Information Resources Management Journal*, *18*(4), 1–20.

WTO. (2016). *World Trade Report 2016—Levelling the Trading Field for SMEs*. WTO Publications. https://www.wto.org/english/res_e/booksp_e/world_trade_report16_e.pdf Accessed 20 January 2019.

Wu, J.-H., & Wang, S.-C. (2005). What Drives Mobile Commerce? An Empirical Evaluation of the Revised Technology Acceptance Model. *Information & Management*, *42*(5), 719–729.

Wu, W.-W., Lan, L. W., & Lee, Y.-T. (2011). Exploring Decisive Factors Affecting an Organization's SaaS Adoption: A Case Study. *International Journal of Information Management*, *31*(6), 556–563.

Yang, C. G., & Lee, H. J. (2016). A Study on the Antecedents of Healthcare Information Protection Intention. *Information Systems Frontiers*, *18*(2), 253–263.

Yang, H., & Tate, M. (2012). A Descriptive Literature Review and Classification of Cloud Computing Research. *Communications of the Association for Information Systems*, *31*(2), 35–60.

Yildirim, E., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing Information Security Management in Small-and Medium-sized Enterprises: A Case Study from Turkey. *International Journal of Information Management*, *31*(4), 360–365.

Young, R. F., & Windsor, J. (2010). Empirical Evaluation of Information Security Planning and Integration. *Communications of the Association for Information Systems*, *26*(1).

Yue, W. T., & Cakanyildirim, M. (2007). Intrusion Prevention in Information Systems: Reactive and Proactive Responses. *Journal of Management Information Systems*, *24*(1), 329–353.

Zajonc, R. B. (1968). Attitudinal Effects of Mere Exposure. *Journal of Personality and Social Psychology*, *9*(2), 1–27.

ZDNet. (2015). *The Target Breach, Two Years Later*. https://www.zdnet.com/article/the-target-breach-two-years-later/ Accessed 24 February 2019.

Zellweger, T. (2007). Time Horizon, Costs of Equity Capital, and Generic Investment Strategies of Firm. *Family Business Review*, *20*(1), 1–15.

Zhao, X., Xue, L., & Whinston, A. B. (2013). Managing Interdependent Information Security Risks. Cyberinsurance, Managed Security Services, and Risk Pooling Arrangements. *Journal of Management Information Systems*, *30*(1), 123–152.

Zurich. (2017). *As Many as 875,000 UK SMEs Suffer Cyber Security Breach in the last 12 Months*. https://www.zurich.co.uk/en/about-us/media-centre/general-insurance-news/2017/as-many-as-875000-uk-smes-suffer-cyber-security-breach-in-the-last-12-months Accessed 3 April 2018.

Appendix

A1. Sample Characteristics (Paper B)

Category	Item	Freq.	%	Category	Item	Freq.	%
Gender	Female	102	48.8	***Education***	High School	72	34.4
	Male	107	51.2		College	65	31.1
Age	18-29	30	14.4		Bachelor	22	10.5
	30-39	46	22.0		Master	36	17.2
	40-49	49	23.4		Other	14	6.7
	50-59	56	26.8	***Work Position***	Entry-level	77	36.8
	60-65	28	13.4		Mid-level	128	61.2
					High-level	4	1.9
				Work Experience (in years)	1-5	17	8.1
					6-15	51	24.4
					16-25	52	24.9
					26-50	89	42.6

Figure 16. Descriptive Sample Characteristics

A2. Measurement Items (Paper B)

Item	Abbr.	Description
Controllability	**CON1**	Whether I use different complex passwords is my sole responsibility.
	CON2	It is primarily up to me whether I use a different complex password.
	CON3	I have full control over the use of different complex passwords.
	CON4	The choice of different complex passwords is completely in my control.
Behavioral Intention	**INT1**	I plan to choose different complex passwords for different accounts.
	INT2	I intend to use a unique complex password for each important account.
	INT3	I plan to protect different accounts with different complex passwords.
Psychological Ownership	**PO1**	Data and files I work with professionally/privately are my own.
	PO2	I feel that data I work with professionally/privately is my property.
	PO3	I have a feeling that this data belongs to me.
Response Cost	**RC1**	It would cause me too many problems to assign different complex passwords.
	RC2	I would be discouraged to use different complex passwords because it would be difficult for me to remember them.
	RC3	It would be very tiring for me to use different complex passwords.
	RC4	It would be too time-consuming for me to use different complex passwords.
Response Efficacy	**RE1**	When I use different complex passwords, I protect professional/private data from theft.
	RE2	The use of different complex passwords reduces the probability of data theft.
	RE3	If I use different complex passwords, it is less likely that professional/private data will be misused.
Self-Efficacy	**SE1**	I am sure I have the ability to use different complex passwords.
	SE2	I find it easy to use different complex passwords for different accounts.
	SE3	Using different complex passwords for each important account would be an easy task for me.
Perceived Severity	**SEV1**	If someone guessed my passwords successfully, I would find it a serious problem.
	SEV2	If someone hacked my important email accounts, it would be serious.
	SEV3	If someone got hold of my passwords, it would be serious.
	SEV4	If someone steals my passwords, there could be serious consequences.
Perceived Vulnerability	**VULN1**	I believe that the probability of password theft is high.
	VULN2	I believe that there is a high probability that my password will be guessed.
	VULN3	I think the chance of my password being hacked are high.
	VULN4	I have a feeling that I am at risk from password theft,
All items were measured on a 7-point Likert scale from “strongly disagree” to “strongly agree”		

Table 14. Descriptive Sample Statistics

A3. Measurement Model Validation (Paper B)

	Work Context								Private Context							
	CON	INT	SEV	PO	RC	RE	SE	VULN	CON	INT	SEV	PO	RC	RE	SE	VULN
CON1	**.813**	.166	.245	.179	-.049	.151	.070	.103	**.924**	.0334	.248	.411	-.288	.579	.339	-.221
CON2	**.852**	.232	.241	.174	-.060	.218	.062	.057	**.919**	.350	.299	.458	-.280	.614	.323	-.217
CON3	**.933**	.431	.241	.118	-.334	.242	.300	-.033	**.900**	.335	.193	.333	-.386	.427	.434	-.189
CON4	**.950**	.423	.256	.153	-.305	.257	.294	-.044	**.922**	.319	.172	.387	-.356	.492	.379	-.231
INT1	.350	**.937**	.361	.072	-.360	.406	.413	-.021	.369	**.944**	.262	.292	-.424	.333	.496	-.016
INT2	.354	**.951**	.301	.103	-.383	.348	.471	-.002	.305	**.916**	.202	.240	-.344	.341	.404	-.111
INT3	.388	**.968**	.351	.097	-.397	.395	.456	-.025	.349	**.949**	.259	.297	-.471	.350	.530	-.073
SEV1	.234	.362	**.874**	.071	-.129	.323	.348	.097	.214	.240	**.878**	.236	-.101	.313	.131	.106
SEV2	.242	.303	**.907**	.055	-.074	.327	.236	.073	.225	.195	**.898**	.272	-.092	.344	.106	.029
SEV3	.260	.293	**.936**	.058	-.117	.332	.284	.100	.276	.263	**.943**	.331	-.056	.374	.124	.085
SEV4	.254	.316	**.906**	029	-.133	.326	.260	.097	.193	.240	**.914**	.261	-.048	.288	.137	.126
PO1	.141	.087	.010	**.869**	-.103	-.020	.027	.160	.407	.211	.205	**.859**	-.143	.404	.277	-.072
PO2	.139	.036	.034	**.933**	-.025	-.081	-.012	.161	.403	.295	.321	**.931**	-.220	.378	.330	-.052
PO3	.174	.129	.107	**.951**	-.011	-.048	.024	.203	.378	.296	.299	**.921**	-.170	.430	.296	-.059
RC1	-.234	-.370	-.081	-.043	**.910**	-.219	-.601	.253	-.318	-.386	-.086	-.192	**.920**	-.096	-.697	.364
RC2	-.223	-.367	-.090	-.039	**.913**	-.193	-.628	.218	-.333	-.423	-.082	-.166	**.946**	-.039	-.734	.337
RC3	-.209	-.332	-.118	-.067	**.945**	-.201	-.605	.186	-.328	-.382	-.050	-.205	**.945**	-.037	-.674	.345
RC4	-.244	-.396	-.172	-.027	**.914**	-.208	-.603	.211	-.337	-.460	-.079	-.180	**.911**	-.087	-.671	.284
RE1	.282	.405	.359	-.005	-.265	**.913**	.408	-.060	.524	.337	.333	.421	-.044	**.912**	.168	-.116
RE2	.181	.376	.324	-.092	-.156	**.913**	.313	-.057	.571	.376	.382	.445	-.085	**.935**	.194	-.165
RE3	.209	.283	.279	-.051	-.170	**.862**	.310	-.046	.461	.252	.248	.319	-.059	**.846**	.140	-.190
SE1	.176	.404	.313	-.048	-.454	.378	**.833**	-.133	.345	.393	.110	.321	-.569	.218	**.840**	-.199
SE2	.194	.411	.254	.009	-.619	.324	**.885**	-.078	.381	.501	.140	.317	-.697	.179	**.940**	-.165
SE3	.251	.423	.266	.076	-.670	.321	**.921**	-.096	.351	.486	.118	.263	-.740	.116	**.917**	-.203
VULN1	.081	.054	.155	.203	.101	.034	.024	**.833**	-.221	-.077	.045	-.070	.331	-.110	-.201	**.880**
VULN2	-.119	-.140	-.071	.071	.329	-.125	-.241	**.707**	-.209	-.134	.070	-.043	.343	-.183	-.205	**.881**
VULN3	.017	-.065	.035	.103	.264	-.030	-.147	**.824**	-.157	-.085	.118	-.030	.266	-.140	-.137	**.871**
VULN4	-.062	.056	.090	.139	.168	-.148	-.133	**.741**	-.230	-.034	.116	-.098	.281	-.155	-.169	**.861**

Table 15. Discriminant Validity (cross-loadings)

A4. Multi-Group Analysis (Paper B)

	Hypotheses		Path Coefficients		PLS-MGA
			Work	Private	p-value
Psychological Ownership	**H2a**	**PO → VULN**	0.192*	-0.067	**0.034**
	H2b	**PO → SEV**	0.06	0.306***	**0.995**
	H2c	**PO → RE**	-0.054	0.446***	**1.000**
	H2d	**PO → RC**	-0.047	-0.199***	**0.062**
	H2e	**PO → SE**	0.015	0.333***	**1.000**
	H2f	**PO → CON**	0.167**	0.437***	**0.998**
Behavioral Intention	H1a	VULN → INT	0.061	0.078	0.552
	H1b	SEV → INT	0.140+	0.094	0.322
	H1c	RE → INT	0.189**	0.268***	0.773
	H1d	RC → INT	-0.173*	-0.223***	0.332
	H1e	SE → INT	0.195*	0.298***	0.786
	H1f	**CON → INT**	0.208*	0.007	**0.044**

Table 16. Multi-Group Analysis (supported hypotheses in bold)

A5. Literature Overview (Paper C)

		Decision Approach			Research Methodology					5 Phase Model	Considered Contextual Aspects											Sample/Audience					Investment Focus			Investment Nuance				SME Focus
					Empirical						Behavioral/ Cognitive		Organizational			Economic			Environmental																
Ref.	Author (Year)	normative	descriptive	prescirptive	modelling, simulation	panel data, survey	experiment	qualitative (interviews, case study)	conceptual/meta-study	Considered Phase(s)	Behavioural Aspects (e.g., Biases,	Cognitive Factors (e.g., knowledge, risk attitude)	Resources and Business Needs	Strategy and Culture	Processes and Structure	Budgeting, Cost-Benefit Analyses	Performance Measures (ROI, value estimation)	Economic Incentives (IT security as profit center)	Information Sharing	Macro-Environmental Factors	Micro-Environmental Factors	decision maker non-IT	decision-maker IT	provider	employees	company level	specific	conceptual/generic	not investement specific	Adoption Y/N (whether)	Area/Content (what)	Source/Origin (from where/whom)	Level/Extent (how much)	
36	Altinkemer and Wang (2011)	x	x		x					2,3,4					x				x	x	x				x				x			x	
56	Baker et al. (2007)		x						x	2.4			x		x	x														x		x	
57	Barnard and von Solms (2000)	x							x	3,4,5			x		x						x	x						x		x			
58	Baskerville (1993)								x	4.5						x	x					x											
4	Bodin et al. (2005)		x		x				x	3.4		x	x			x	x					x				x			x		x		
37	Cavusoglu et al. (2008)	x			x				x	(3),4				x			x					x				x					x		
2	Cavusoglu et al. (2004)	x			x					4, 5							x					x			x						x		
3	Cavusoglu et al. (2015)		x			x				4		x	x	x						x	x		x			x			x		x		
20	Dor and Elovici (2016)		x					x		4	x	x	x	x	x	x				x	x	x				x				x			
38	Dutta and Roy (2008)		x		x					4	x	x	x		x							x			x				x				
39	Ekenberg et al. (1997)	x			x				x	2,3,4		x										x	x					x					
40	El-Gayar and Fritz (2010)		x	x	x				x	3.4	x	x	x									x	x					x					
62	Fenz et al. (2011)		x					x	x	2,3,4,5		x	x			x						x					x			x		x		
41	Fielder et al. (2016)	x			x			x		4			x				x													x		x	x
42	Finne (1998)	x			x					2,3,4		x												x				x					
43	Gordon and Loeb (2002)	x			x					4			x			x	x						x				x				x		
44	Grossklags et al. (2008)	x			x					4				x	x		x						x			x			(x)			x	
45	Guarro (1987)		x		x				x	2,3,(4)			x			x							x							x			
46	Gupta et al. (2006)	x			x				x	3, 4, 5			x		x	x							x					x					
47	Herath and Herath (2008)	x			x					4, 5						x						x	x			x	x		x	x		x	
10	Huang et al. (2014)	x			x					(2),4			x			x	x	x		(x)						x				x		x	
6	Khansa and Liginlal (2009)	x			x					4.5						x		x	x	x				x		x						x	
48	Kim and Lee (2007)	x			x			x		3.4														x		x	x	x		x	x		
49	Kolfal and Patterson (2013)	x			x					3.4						x	x		x		x					x					x		
59	Kwok and Longley (1999)		x						x	2,3,4			x		x					x						x				x			
33	Lee et al. (2011)	x			x	x				4						x	x			x	x					x				x		x	
31	Lee and Larsen (2009)		x			x				4	x	x	x			x					x	x	x				x			x			x
50	Liu et al. (2011)	x			x					4							x		x					x		x				x			
51	Miller et al. (2016)		x		x		x			2,3, (4)						x						x						x					
52	Nazareth and Choi (2015)	x			x					2,3,4,5			x		x	x									x				x		x		
60	Purser (2004)		x						x	4.5			x	x			x			x						x				x		x		
55	Qian at al. (2012)		x					x		4		x	x		x	x										x			x					
53	Rees et al. (2011)	x			x				x	2,3,4						x	x					x	x				x			x		x	
54	Ryan and Ryan (2006)	x			x					4.5						x	x									x			x				
34	Sawik (2013)	x			x					3.4		x				x							x			x				x		x	
14	Straub and Welke (1998)		x					x	x	1,2,3,4,5	x	x	x		x	x											x				x			
35	Wang et al. (2008)	x			x			x		4.5		x		x		x	x					x	x				x				x		
61	Wood (1988)		x						x	1,2,3,(4)	x	x	x	x		x							x					x					
63	Young and Windsor (2010)		x			x				2,3,4		x			x	x							x				x				x		
SUM		22	17	1	25	4	1	7	15	N/A	6	15	20	7	12	24	15	2	3	8	6	11	20	4	1	13	8	20	8	6	21	1	19	2

Table 17. Literature Overview

A6. Literature Search Process (Paper E)

Search Term Example	*tak (IT-security OR IT security OR information security OR cyber security OR data security OR securing information assets OR technology security OR InfoSec OR InfSec OR secur* OR protect*) AND src (Journal of Strategic Information Systems)*							
	EJIS	**ISJ**	**ISR**	**JAIS**	**JIT**	**JMIS**	**JSIS**	**MISQ**
Abstract (n=320)	34	21	50	25	23	82	17	68
Articles remaining after Title Screening (exclusion criteria: publication type (editorials, books); topics (knowledge management, open source software, corporate wikis, etc.))								**199**
Articles remaining after Abstract Screening (exclusion criteria: domain (technical, legal, general); topics (eCommerce, SNS, end-user behavior))								**105**
Articles remaining after Clustering and Full Text Screening (exclusion criteria: sample (employees, end users); topics (employee misconduct, policy and compliance))								**28**
Articles after Forward and Backward Search within the Basket of Eight								**29**
tak = title, abstract, and keywords; src = source								

Table 18. Overview of the Literature Search Process based on Vom Brocke et al. 2009

Additionally, we screened peer-reviewed publications in the databases provided by ScienceDirect (title, abstract, keywords) and ACM Digital Library (abstract), and the AIS Library (AISeL) (title, subject, abstract) via the search term "SME OR (small and medium) OR (start up) OR startup AND security" and variations of the term. Our AISeL search only resulted in a total of 12 unique articles, ACM Digital Library in 24 articles, and ScienceDirect offered a total of 72 articles. After a title screening and only including peer-reviewed articles, 23 article abstracts were screened. The full text of only 10 papers was screened resulting in a total of 6 papers after back and forward search which could be used for a supplementary review.

A7. Overview of organizational IT security studies (Paper E)

					Investment Decision		SME Context	
Author/s (Year)	**Journal**	**Method**	**Theory/ Model**	**Sample/Study Context**	**Focus**	**Consideration**	**Focus**	**Consideration**
Angst et al. (2017)	MISQ	Quantitative	Institutional Theory	US hospitals	●	Antecedent	◐	SME included in sample; effect of hospital size
Baskerville (1991)	EJIS	Conceptual		-	◐	Outcome	○	-
Cavusoglu et al. (2008)	JMIS	Modelling	Game Theory, Decision Theory	-	●	Outcome	○	-
Chen et al. (2011)	MISQ	Modelling	Queuing Theory	-	◐	Antecedent	○	-
Dhillon and Backhouse (2001)	ISJ	Review	-	-	○	-	○	-
Dhillon and Torkzadeh (2006)	ISJ	Qualitative	Value-focused Thinking	US managers from various industries with IT experience	◐	Outcome	◐	SME included in sample; no discussion of org. size differences
Gal-Or and Ghose (2005)	ISR	Modelling	Game Theory	-	●	Outcome	◐	Indirect consideration of firm size
Gordon et al. (2010)	MISQ	Quantitative	Market-Value Relevance Model	> 20000 US firms, various sizes and industries	○	-	◐	SME potentially included in sample; no discussion of org. size differences
Herath and Herath (2008)	JMIS	Quantitative	Real Options Model	Mid-sized US university	●	Object of Evaluation	○	-
Hsu et al. (2012)	ISR	Mixed Method	Institutional Theory	Large Korean companies	●	Outcome	○	-
Hsu (2009)	EJIS	Qualitative	(Technological) Frames Analysis	Large Taiwanese financial institution	○	-	○	-
Hu et al. (2007)	JSIS	Qualitative	(Neo-)Institutional Theory	Large multi-national enterprise	◐	(ind.) Outcome	○	-
Hui et al. (2012)	JMIS	Modelling	Principal-Agent Theory	-	◐	(ind.) Antecedent	○	-
Kumar et al. (2008)	JMIS	Modelling	Financial Asset Valuation	-	●	Antecedent	○	-
Kwon and Johnson (2014)	MISQ	Quantitative	Organizational Learning	2386 organizations in US healthcare	●	Antecedent	◐	SME potentially included in sample
Lee and Larsen (2009)	EJIS	Quantitative	Protection Motivation Theory	239 US SMB executives	●	Outcome	●	SME sample, no in-depth analysis of SME characteristics
Lee et al. (2013)	ISR	Modelling	Principal-Agent, Game Theory	-	◐	Antecedent	◐	Context relevant for SME, but not explicitly stated

					Investment Decision		SME Context	
Author/s (Year)	**Journal**	**Method**	**Theory/ Model**	**Sample/Study Context**	**Focus**	**Consideration**	**Focus**	**Consideration**
Sen and Borle (2015)	JMIS	Modelling	Opportunity Theory of Crime	Secondary data from multiple sources, e.g., US Bureau of Economic Analysis, Secunia	●	Antecedent	○	-
Siponen (2005)	EJIS	Review	Analytical Framework	-	◐	-	○	-
Spears and Barki (2010)	MISQ	Mixed Method	User Participation in Security Risk Management	IS professionals across US organizations of various sizes and industries	○	-	◐	SME potentially included in sample; scales assume larger firms,
Straub (1990)	ISR	Mixed-Method	General Deterrence Theory	IS managers, security officers and internal auditors; 1211 US organizations of various sizes and industries	◐	(ind.) Antecedent	◐	SME potentially included in sample; no differences between SME and large firms discussed
Straub and Welke (1998)	MISQ	Qualitative	General Deterrence Theory	2 large US companies	◐	Outcome	○	-
Sun et al. (2006)	JMIS	Modelling	Theory of Belief Functions	Application based on assurance results of a global company	◐	(ind.) Outcome	○	-
Wang et al. (2008)	ISR	Quantitative	Extreme Value Analysis	Large financial institution	●	Antecedent	○	-
Wang et al. (2013)	ISR	Mixed-Method	Disclosure Theory	62 publicly traded companies	○	-	○	-
Wolff (2016)	JMIS	Conceptual	Duality of Technology	-	○	-	○	-
Yue and Cakanyildirim (2007)	JMIS	Modelling	Optimal Control Approach	-	○	-	○	-
Zhao et al. (2013)	JMIS	Modelling	Alternative Risk Transfer	-	●	Antecedent	○	-

EJIS = European Journal of Information System; **ISJ** = Information Systems Journal; **ISR** = Information Systems Research; **JAIS** = Journal of the Association for Information Systems; **JIT** = Journal; **JMIS** = Journal of Management Information; Systems; **JSIS** = Journal of Strategic Information Systems; **MISQ** = MIS Quarterly

● = distinct, clear, focal
◐ = semi-distinct, indirect
○ = not distinct, not focal

ind. = indirect

Table 19. Overview of organizational IT security studies in the Senior Scholars' Basket of Journals (SenS-8)

A8. Interview Guide (Paper E)

The initial interview guide covered 5 key areas and served as a coarse guideline during the interviewing process. Below are some selected questions which were continuously modified or deepened according to the respective interviewees, their role, or background (e.g., managing director or consultant, provider or user firm, IT or business background). In order to ensure that interesting new ideas could be spontaneously pursued or to account for the particular interview context, each interview was unique and would differ from previous or subsequent ones.

Key Area	Exemplary Questions
(1) Company Profile	Please provide a short description of your company and role.
	What role does IT generally play for your company? Could you operate without IT?
	What is your general understanding of corporate, information, and IT security?
(2) IT Security Status Quo	How would you rate the IT security awareness in your company?
	How is this awareness distributed when one distinguishes between management, IT and employees?
(3) Processes and Assessments	How do you decide upon IT security investments?
	Have you already experienced a bad investment in the area of IT security?
	Do you use specific tools/models when making IT investment decisions?
(4) Stakeholder Perspective	Which kind of external support do you consider regarding IT security investments?
	Which kind of external support do you consider regarding IT security implementation?
	What's your take on legal regulations, which enforce IT security investments, e.g. data protection regulation or the IT security law?
(5) Need for Action	What need for action do you see in the area of IT security, especially for SME?
	What kind of support would you like? Who should offer them?

Table 20. Interview Questions