Information Systems Frontiers (2019) 21:1285–1305
https://doi.org/10.1007/s10796-019-09959-1

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

Margareta Heidt[1] · Jin P. Gerlach[1] · Peter Buxmann[1]

Published online: 9 November 2019

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

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 and 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 2018) 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 (Straub and Welke 1998; J. Wang et al. 2008; Coden et al. 2016; Angst et al. 2017). This attention also manifests itself in increasing IT security investments likely to exceed 124 billion USD in 2019 according to research company Gartner (Moore and Keen 2018). 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%) of British SME, for example, plan to spend less than 1000 GBP on cyber security measures despite seeing themselves

✉ Margareta Heidt
heidt@is.tu-darmstadt.de

Jin P. Gerlach
gerlach@is.tu-darmstadt.de

Peter Buxmann
buxmann@is.tu-darmstadt.de

[1] Technische Universität Darmstadt, Hochschulstraße 1, D-64289 Darmstadt, Germany

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. 2012) or focus on specific industry sectors such as healthcare or finance (Kwon and Johnson 2014; J. Wang et al. 2008, Yang and Lee 2016). Consequently, this suggests that the majority of all companies might have been overlooked since SME make up over 90% 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 (Ballantine et al. 1998; Arendt 2008; 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 and 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 and 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.

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 and 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 2016; 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.

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.

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; Sen and Borle 2015; Chen et al. 2011; Gal-Or and Ghose 2005; Hui et al. 2012; Kumar et al. 2008; Lee et al. 2013; Yue and Cakanyildirim 2007; Zhao et al. 2013), or review extant literature (Dhillon and Backhouse 2001; Siponen 2005). Only a total of fourteen papers followed either a qualitative approach (Dhillon and Torkzadeh 2006; Hsu 2009; Hu et al. 2007; Straub and Welke 1998), conducted a quantitative/empirical study (Angst et al. 2017; Gordon et al. 2010; Herath and Herath 2008; Kwon and Johnson 2014; Y. Lee and Larsen 2009; J. Wang et al. 2008), or pursued a combined, mixed-method approach (Hsu et al. 2012; T. Wang et al. 2013; Spears and Barki 2010; Straub 1990). Out of these, only one study exhibits a distinct SME focus through their sample (Lee and Larsen 2009) whereas two other study samples explicitly contain SME (Angst et al. 2017; Dhillon and Torkzadeh 2006) and several others only potentially include SME since they omit detailed or clear sample characteristics (Gordon et al. 2010; Kwon and Johnson 2014; Spears and Barki 2010; Straub 1990).

With the exception of Angst et al. (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 et al. (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 and 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., Iacovou et al. 1995; Thong 1999; Forman 2005). 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 and Demirguc-Kunt 2006; Caldeira and Ward 2003; H. Chen et al. 2007; Dholakia and 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; US Small 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 and Park 2016; Ng and Feng 2006) whereas the other half was split into one qualitative empirical study focusing on current trends (Keller et al. 2015) 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. (2016) 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 (Cragg et al. 2011; Caldeira and Ward 2003) to build a framework and to derive propositions on how these identified characteristics affect organizational IT security investments in SME.

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

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% of all firms globally (WTO 2016). In the non-financial sector, SME even represent 99.7% of all firms in the OECD area while accounting for 60% 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 and Evrard 1999; Verhees and 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 and Irani 2003; Wielicki and Arendt 2010; Cragg et al. 2011). 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.

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 (1998). 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 Fig. 1 represents a condensation of extant models and examinations performed by various researchers and practitioners (Boyes and Irani 2003; Caldeira and Ward 2003; Dojkovski et al. 2007; Chang and Wang 2011; Cragg et al. 2011; OECD 2017):

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 and 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 and 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 Fig. 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 and Vrazalic 2005). Previous SME research finds that leadership characteristics of the

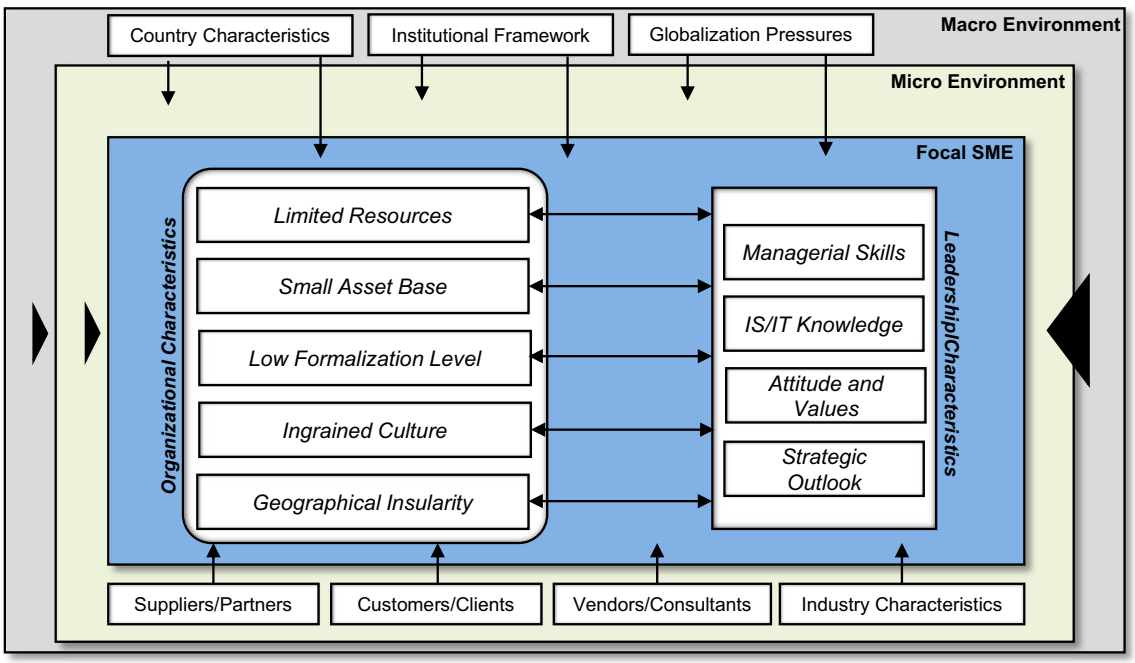

Fig. 1 Conceptual Framework of SME Constraints

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 and 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 and 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 and 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 and 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 and 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 (Fishbein and Ajzen 1975; Ajzen 1991; Angst et al. 2017). 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 and 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 and 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 and 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 (Thong and Yap 1995; Thong 1999; Caldeira and Ward 2003). Drawing on Caldeira and Ward's (2003) findings, a follow-up study on organizational IS competences in SME by Cragg et al. (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., Fishbein and Ajzen 1975; Ajzen 1991; Riemenschneider et al. 2003; Dwivedi et al. 2017). Since extant organizational IT security research confirms that managers' concern over systems security vary according to their individual characteristics and *Values* (Goodhue and 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 (Feeny and Willcocks 1998; Drechsler and Weißschädel 2018; Bassellier et al. 2001). 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). 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.

4 Qualitative Study

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?").

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 and 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%) are active in the service sector while 24% of the sample organizations provide a mixture of services and manufactured goods, 8 % 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 1.

All interviews (length average of 72 min) 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).

Table 1 Participant Overview

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 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 (1–9 employees); *s* small (10–49 employees), *m* medium (50–249 employees)

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 literature (e.g., Albrechtsen 2007). Coding cycles were used to answer our research questions as displayed in Fig. 2 following the suggested techniques of Miles et al. (2013).

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 and 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 and

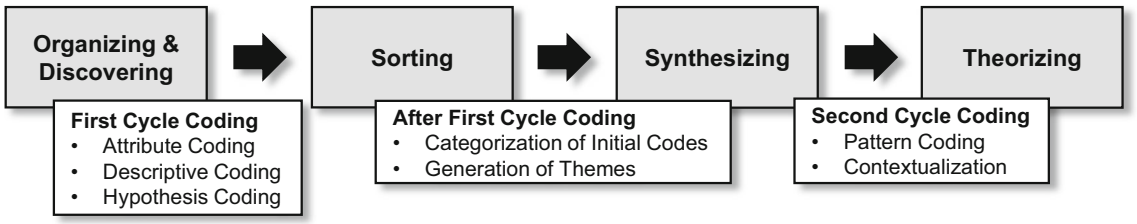

Fig. 2 Analysis Technique

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 and 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 et al. (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.

4.4 Results

The propositions stated in 3.2. and the visualized influence of SME characteristics (Fig. 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.

4.4.1 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: [1] SME do not employ 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 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*

4.5 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.

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 and 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 and 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 (Cragg et al. 2013; Bradshaw 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.

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 and 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 and 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.

Acknowledgements 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".

Appendix

Table 2 Overview of the literature search process based on Vom Brocke et al. 2009

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

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.

Table 3 Overview of organizational IT security studies in the Senior Scholars' Basket of Journals (SenS-8)

					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
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,
					Investment Decision		**SME Context**	
Author/s (Year)	**Journal**	**Method**	**Theory/ Model**	**Sample/Study Context**	**Focus**	**Consideration**	**Focus**	**Consideration**
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 4 Interview Questions

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?

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.

References

Agell, J. (2004). Why are small firms different? Managers' views. *Scandinavian Journal of Economics, 106*(3), 437–453.

AIS (2016). Senior Scholars' Basket of Journals. Association for Information Systems (AIS). https://aisnet.org/?SeniorScholarBasket. Accessed 20 January 2019.

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

Albrechtsen, E. (2007). A qualitative study of Users' view on information security. *Computers & Security, 26*(4), 276–289.

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

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.

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.

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

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*(4), 241–251.

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. (1991). Risk analysis: An interpretative feasibility tool in justifying information systems security. *European Journal of Information Systems, 1*(2), 121–130.

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). Thousand Oaks: Sage.

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.

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.

Bogdan, R. C., & Biklen, S. K. (2007). *Qualitative research for education: An introduction to theories and methods* (Vol. 5). Boston: Pearson Education.

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

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.

Buckley, P. J. (1997). International technology transfer by small and medium-sized enterprises. *Small Business Economics, 9*(1), 67–78.

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

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.
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., 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.
Chell, E., Haworth, J. M., & Brearley, S. A. (1991). *The entrepreneurial personality. Concepts, cases, and categories (Vol. 1, Routledge small business series)*. London: Routledge.
Chen, H., Lee, M., & Wilson, N. (2007). Resource Constraints Related to Emerging Integration Technologies Adoption: The Case of Small and Medium-Sized Enterprises. In Proceedings of the 13th Americas Conference on Information Systems, Keystone, Colorado.
Chen, P., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. *MIS Quarterly, 35*(2), 397–A393.
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 20 February 2019.
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.
Creswell, J. W. (1998). *Qualitative inquiry and research design: Choosing among five traditions*. London: Sage.
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.
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, St Gallen, Switzerland.
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.
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.
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). In European Commission (Ed.): Official Journal of the European Union 46 (L 124).
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.
Feeny, D. F., & Willcocks, L. P. (1998). Core IS Capabilities for Exploiting Information Technology. Sloan Management Review (9–21).
Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems, 86*(3), 13–23.
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*. Reading: Addison-Wesley.
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). Thousand Oaks: Sage.
Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. *Information Systems Research, 16*(2), 186–208.
Goffman, E. (1959). *The presentation of self in everyday life*. London: Penguin.
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 voluntary disclosures concerning information security. *MIS Quarterly, 34*(3), 567–594.
Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History.
Greener, S. (2008). *Business research methods*. London: Ventus Publishing ApS.
Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly, 30*(3), 611–642.
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.
Hermanns, H. (2004). Interviewing as an activity. In U. Flick, E. von Kardoff, & I. Steinke (Eds.), *A companion to qualitative research* (pp. 209–213). London: Sage.
Howorth, C. (2001). Small firms demand for finance: A research note. *International Small Business Journal, 19*(4), 78–86.
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.
Hsu, C. W., Lee, J. N., & Straub, D. W. (2012). Institutional influences on information systems security innovations. *Information Systems Research, 23*(3), 918–939.
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.
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.
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*. Thousand Oaks: Sage.

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/. Accessed 12 March 2018.

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information security threats and practices in small businesses. *Information Systems Management, 22*(2), 7–19.

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.

Kwon, J., & Johnson, M. E. (2014). Proactive versus reactive security Investments in the Healthcare Sector. *MIS Quarterly, 38*(2), 457–471.

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, 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.

Lowry, P. B., Moody, G. D., Gaskin, J., Galletta, D. F., Humphreys, S. L., Barlow, J. B., et al. (2013). Evaluation journal quality and the Association for Information Systems Senior Scholars' journal basket via bibliometric measures: Do expert journal assessments add value? *MIS Quarterly, 37*(4), 993–1012.

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.

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.

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.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Beverly Hills: Sage.

Miles, M. B., Huberman, A. M., & Saldana, J. (2013). *Qualitative data analysis. A methods sourcebook (Vol. 3)*. Los Angeles: Sage.

Mintzberg, H. (1989). The Structuring of Organizations. In: Readings in Strategic Management (pp. 322–352). London: Palgrave.

Moore, S., & Keen, E. (2018). 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.

Morse, J. M. (1994). *Designing funded qualitative research*. Thousand Oaks: Sage.

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.

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.

OECD. (1997). *Small businesses, job creation and growth: Facts, obstacles and best practices*. Paris: OECD Publishing.

OECD. (2005). *Glossary of statistical terms - small and medium-sized enterprises (SMEs)*. Paris: OECD Publishing.

OECD. (2016). *Financing SMEs and entrepreneurs: An OECD scoreboard. Definition of SMEs in China*. Paris: OECD Publishing.

OECD. (2017). *Small, medium, strong. Trends in SME performance and business conditions*. Paris: OECD Publishing.

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.

Piscitello, L., & Sgobbi, F. (2004). Globalisation, E-business and SMEs: Evidence from the Italian District of Prato. *Small Business Economics, 22*(5), 333–347.

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.

Rogers, R. (1983). Cognitive and physiological processes in fear-based attitude change: A revised theory of protection motivation. In C. J & R. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–176). New York: Guilford Press.

Saldaña, J. (2009). *The coding manual for qualitative researchers*. London: Sage.

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.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 32*(2), 314–341.

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.

Sonnenschein, R., Loske, A., & Buxmann, P. (2017). The Role of Top Managers' IT Security Awareness in Organizational IT Security Management. In Proceedings of the 38th International Conference on Information Systems, Seoul, 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. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255–276.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441–469.

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.

Teo, T. L., Chan, C., & Parker, C. (2004). Factors Affecting e-Commerce Adoption by SMEs: A Meta-Analysis. In Proceedings of the Australasian Conference on Information Systems, Hobart, Australia.

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.

United Nations (2008). International Standard Industrial Classification of All Economic Activities, Rev.4. In United Nations Division (Ed.). New York.

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.

USITC (2010). Small and Medium-sized Enterprises: Overview of Participation in U.S. Exports. Investigation No. 332–508 (Vol. 4125). Washington: USITC Publication.

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.

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, Vienna, Austria.

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.

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. A. (2015). Multi-theoretical literature review on information security investments using the resource-based view and the organizational learning theory. In Proceedings of the 36th International Conference on Information Systems, Fort Worth, USA.

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.

Wolcott, H. F. (1994). *Transforming qualitative data: Description, analysis, and interpretation*. Thousand Oaks: Sage.

Wolff, J. (2016). Perverse effects in defense of computer systems. When more is less. *Journal of Management Information Systems, 33*(2), 597–620.

World Economic Forum (2019). The Global Risks Report 2019. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf. Accessed 14 February 2019.

WTO (2016). World Trade Report 2016 - Levelling the Trading Field for SMEs. Geneva: WTO Publications. https://www.wto.org/english/res_e/booksp_e/world_trade_report16_e.pdf. Accessed 20 January 2019.

Yang, C. G., & Lee, H. J. (2016). A study on the antecedents of healthcare information protection intention. *Information Systems Frontiers, 18*(2), 253–263.

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.

Yue, W. T., & Cakanyildirim, M. (2007). Intrusion prevention in information systems: Reactive and proactive responses. *Journal of Management Information Systems, 24*(1), 329–353.

ZDNet (2015). The Target Breach, Two Years Later. https://www.zdnet.com/article/the-target-breach-two-years-later/. Accessed 24 February 2019.

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.

Margareta Heidt is a doctoral candidate at the School of Business, Economics, and Law, Technische Universität Darmstadt, Germany. She received her M.Sc. in International Business Management from Philipps-Universität Marburg and INSEEC Business School Paris in 2014. After working in the SaaS industry, she pursued her doctoral research in the field of organizational decision-making with a focus on Cloud Computing adoption and IT security investment.

Jin P. Gerlach is an assistant professor of MIS at the School of Business, Economics, and Law, Technische Universität Darmstadt. His research interests include the adoption and use of IS at the individual level, organizational management of IS security and privacy, and data-driven value creation within organizations. His work has been published in MIS Quarterly, Journal of the AIS, Journal of Strategic Information Systems, and other outlets.

Peter Buxmann is Full Professor of Information Systems at Technische Universität Darmstadt, Germany. He holds a Ph.D. in general management and Information Systems from Frankfurt University. His main research areas are the digitalization of business and society, methods and applications of artificial intelligence, entrepreneurship and the development of innovative business models, as well as the economics of cybersecurity and privacy. He has published in several journals, such as Information Systems Research, Journal of Information Technology, Journal of Strategic Information Systems, European Journal of Information Systems, Information Systems Journal, and Journal of Product Innovation Management.